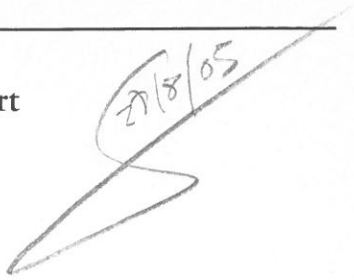
Anti-Hacker Report



Copyright © 2001 by DATA BECKER GmbH & Co. KG
Merowingerstr. 30
40223 Düsseldorf

1. Primera Edición 2001

Revisión David Grosvenor

Traducción LH Servicios Informáticos

Revisión (Edición en en castellano) LH Servicios Informáticos, Roberto García Cáceres

Diseño de cubierta Inhouse-Agentur DATA BECKER

Maquetación MACAYPA S.A.

Impresión MACAYPA S.A.

e-Mail info@databecker-es.com

Reservados todos los derechos. Queda prohibida la reproducción total o parcial de este libro de cualquier forma (impresión, fotocopia u otro procedimiento), así como su copia o difusión mediante el empleo de un método electrónico, sin el consentimiento por escrito de DATA BECKER GmbH & Co.

ISBN 84-95585-15-4
D. L. M-24341-2001

Observaciones importantes

Los procedimientos y programas incluidos en este libro se mencionan sin tener en cuenta el estado de su patente, pues dicha mención está destinada a fines no profesionales y didácticos.

Todos los datos y programas incluidos en este libro han sido cuidadosamente elaborados y compilados por el autor y se han reproducido tras aplicar medidas de control efectivas. No obstante, no podemos excluir la posibilidad de que éste contenga algún error, por lo que DATA BECKER declina toda garantía o responsabilidad jurídica respecto las consecuencias derivadas de una información errónea. En todo caso, el autor atenderá gustoso cualquier comunicación relativa a la existencia de un error.

Cabe señalar, asimismo, que las designaciones de software y de hardware y los nombres de marcas de las diversas empresas suelen estar protegidas por los derechos de marcas y patentes.

Prólogo

Piratas informáticos penetran en Microsoft y roban el código fuente de Windows

Guerra de información en Oriente Próximo

Graves agujeros de seguridad en Internet Explorer facilita el acceso a los hackers

Estos fueron algunos de los titulares en los últimos meses que nos demuestran que los hackers han dejado de ser sólo un mito con aires de Hollywood, para convertirse en la amenaza cotidiana de todo aquél que trabaje con ordenadores.

Este libro intenta ilustrar extensamente el tema de los "hackers", presentando de modo detallado y reproducible tanto los métodos que emplean los piratas informáticos, como las posibilidades de protección frente a sus ataques. Por un lado, pretende que comprenda cómo actúa un hacker y, de esta forma, poder detectar el riesgo potencial para protegerse de él. Por otro lado, tomar las medidas de protección más adecuadas para cada caso y necesidades de seguridad.

El libro va acompañado de un CD-ROM, donde encontrará casi todos los programas que se detallan en el libro. Usted podrá reproducir todos los pasos directamente en un entorno práctico. El CD-ROM posee autoarranque, por lo tanto debería arrancar automáticamente nada más introducirlo. De no ser así, simplemente abra el archivo *index.htm* de forma manual. Este archivo contiene una interfaz donde encontrará descripciones abreviadas de los programas, así como referencias al correspondiente capítulo del libro. Aparte de esto, aquí podrá instalar o arrancar directamente dichos programas.

Aunque en la cubierta sólo figure un autor, es sabido por todos que durante la gestación de un libro, casi siempre, interviene un amplio número de personas, a las que me gustaría mencionar aquí. En primer lugar, doy las gracias a todos los creadores de software que nos han permitido adjuntar sus programas en este libro, agradecimientos que, también, me gustaría dirigir a los numerosos proveedores de ofertas en la red sobre el tema "Hackers" y "Seguridad en el ordenador", que tanto me han ayudado en la recopilación de información. En nombre de todos los colaboradores de la editorial, me gustaría agradecer a David Grosvenor su magnífica cooperación y ayuda en este proyecto. Gracias también a Fritz por las capturas de pantalla y, como siempre, a Lisa por su apoyo moral y su té caliente.

Para finalizar, les deseo que se diviertan con la lectura de este libro y espero que

les resulte útil. También confío en que les proporcione nuevos conocimientos y aclare esas pequeñas dudas que todos tenemos, ayudándoles a proteger su ordenador de los hackers, sus datos y su entorno privado en la red. Si tienen algún tipo de preguntas, observaciones o sugerencias relacionadas con el tema, estaré encantado de resolverlas si me las transmiten personalmente por e-mail. Podrán localizarme en Wolfram.Gieseke@technologist.com.

Wolfram Gieseke, primavera de 2001

Tabla de Contenidos

1. El hacker, ¿Ese ser (des)conocido? 15

1.1 **El robo rápido de datos – anatomía del ataque de un hacker** 19

Paso 1: explorar los objetivos potenciales 19

Paso 2: análisis del objetivo de un ataque 24

Paso 3: la elección del método de ataque 40

1.2 **El ataque al sistema** 41

Sistemas infectados – sabotaje mediante virus informáticos 41

El Gran Hermano te vigila – infiltración de troyanos 42

Puertas traseras – aprovechar los fallos del sistema y los agujeros de seguridad 45

Averiguar contraseñas por la fuerza 47

Control remoto – manipulación de un PC mediante acceso remoto 48

Acceso a sistemas de ficheros desprotegidos 49

Fisgoneo de contraseñas – Password Sniffing 51

Internet, cancha de juego para los hackers 52

Pirateo sin ordenador – Social Hacking 56

1.3 **Chicos malos, "script kids" y saboteadores** 58

Just for fun – chicos con talento que se aburren 59

Rencor y envidia – compañeros de trabajo envidiosos 60

Hackers clásicos – entusiastas e ideólogos 61

Negocios turbios – espionaje y sabotaje 64

Information Warfare – guerra en la era de la información 65

2. Nivel de seguridad 1: ataques locales 67

2.1 **Entrada a través del botón de conexión** 69

Contraseñas BIOS – ¿protección o agujero de seguridad? 69

2.2 **El administrador de usuarios de Windows** 75

Definir nuevos perfiles de usuario 79

¿Hasta dónde es seguro el administrador de usuarios? 82

Un verdadero control de acceso con eSafe 85

2.3 **El salvapantallas – una trampa de seguridad** 94
Así de segura es la contraseña del salvapantallas 97
2.4 **Protección por contraseña para el PC y los datos** 101
La importancia de las contraseñas 101
Así son seguras las contraseñas 103
Síntomas de que la contraseña ha sido pirateada 109
Contraseñas en aplicaciones y documentos 111
2.5 **Ataques al ordenador por hardware** 114
Señales ópticas y acústicas 115
Radiación electromagnética 116
Interceptar el cable mediante sobreacoplamiento 120

3 Nivel de seguridad 2: peligros procedentes de Internet ..... 1'

3.1 **El navegador web: una fuente de riesgo. Qué puede suceder** .....
Los peligros del PC conectado 126
Peligros online en el ámbito privado 126
Peligros online para su bolsillo 127
3.2 **Conceptos de seguridad – las funciones protectoras de los navegadores** 127
Zonas y niveles de seguridad en Internet Explorer 135
Las opciones avanzadas de seguridad de Internet Explorer 139
Las funciones de seguridad de Netscape Navigator 146
Peligros causados por agujeros de seguridad 151
3.3 **Un PC teledirigido – los peligros del ActiveX, JavaScript & Co.** 152
Utilidad y riesgos de los contenidos activos en páginas web 153
Desactivación fiable de los componentes ActiveX 156
Impedir la ejecución de Java-Applets 160
Peligros causados por scripts dinámicos 166
Medidas de prevención con los Plug-Ins 168
3.4 **Virus y troyanos – protección contra infecciones digitales** 169
Protección eficaz contra los virus 173
Escáner antivirus – ¿Doy positivo? 185
Espías en la sombra – los caballos de Troya 191
Cuarentena – verificar cuidadosamente el software nuevo 191

4. Nivel de seguridad 3: protección contra intrusos 203

4.1 Un muro de protección contra los atacantes – Firewalls 203
Principio funcional: filtraje regulado del tráfico de datos 204
Soluciones profesionales frente a los firewalls personales 206
Sencillo y seguro: ZoneAlarm, para usuarios noveles 207
Flexible y potente: eSafe para usuarios avanzados 221

4.2 La confianza está bien, el control aún mejor – vigilar el ordenador 248
Controlar los ataques y otras actividades 249
Vigilancia automática de PCs no custodiados 259

5. Contraataque – ¡Defiéndase! 267

5.1 ¡Abajo la máscara! – identificar al atacante 268
Ping – ¿Quién eres? 268
Traceroute – ¿De dónde vienes? 271
Whois – descubrir a los que están detrás 272
NeoTrace – análisis profesional 276

5.2 Si ya hemos agotado todos los recursos – ¿Devolvemos el golpe? 283
Ojo por ojo, diente por diente 283
Soluciones online para luchar contra los hackers 284
HackTracer – bloquear y denunciar a los hackers 286

5.3 Recursos legales contra los hackers 295
Persecución por vía penal 295
Persecución por vía civil 296

6. Peligros en la red – ataques dentro de la red de empresa 299

6.1 Ataques a PCs integrados en una red 300
Puertos abiertos – invitaciones para los hackers 301
¿Quién me está espiando? – software para detectar un ataque 309

6.2 Atacar el tráfico de datos dentro de la red 315
Fisgoneo de contraseñas y datos confidenciales – Sniffing de paquetes 315

6.3 **Vigilancia en el puesto de trabajo – ¿Qué es factible y está permitido?** 321
Posibilidades técnicas para la vigilancia 322
¿Justicia ante todo? – esto es lo que el jefe tiene derecho a saber sobre usted 322
Las reglas de oro – así debe actuar 325
6.4 **Borrar las huellas delatoras de su navegación por Internet** 326
Borrar el caché y los datos de historial del navegador 327
Proteger las contraseñas privadas en el puesto de trabajo 338
Datos privados confidenciales en el puesto de trabajo 342
6.5 **Windows en la red: una combinación peligrosa** 345
El uso compartido de archivos e impresoras 345
Los protocolos de red: una fuente de peligros 354
El Servidor de acceso telefónico a redes como vía de invasión 359

7 E-Mail: arma, fuente de información y medio de comunicación 363

7.1 **El e-mail como arma – ataques por correo electrónico** 365
Remitente desconocido – borrar las huellas del e-mail 365
Bajo bandera falsa – falsificar el remitente del e-mail 370
Bombas virtuales – paralizar sistemas mediante correo electrónico 375
Virus de e-mail, ¡no, gracias! – la configuración del programa de correo electrónico 381
7.2 **El correo electrónico como fuente de información – los riesgos de la correspondencia electrónica** 390
Postales electrónicas – por eso las puede leer cualquiera 390
¿Cuánto se espía realmente? 394
Contramedidas: encriptar los mensajes 397
Así se revientan las claves 402
7.3 **Lectores encubiertos, ¡no, gracias! – encriptar un e-mail con PGP** 404
Las herramientas de PGP 404
Distribuir las claves propias PGP 412
Incluir claves públicas 415
Leer mensajes encriptados 420

Firmar mensajes ... 421
Emplear PGP con cualquier aplicación ... 424
La encriptación de archivos adjuntos ... 429
¿Hasta qué punto es fiable PGP? ... 430
S/MIME – la alternativa de pago ... 430
7.4 Ocultar en lugar de desencriptar – protección mediante esteganografía ... 433
La idea: ocultar información confidencial entre masas de datos ... 434
Volver visibles los datos ocultos ... 440
7.5 Freemailer – gratuitos, pero no exentos de peligro ... 443
GMX & Co. – servicios de correo electrónico a través de la Red ... 444
Más vale prevenir – las reglas más importantes a seguir con los servicios de freemail ... 446
Una dirección para cada asunto – aprovechar las direcciones gratuitas de correo electrónico 448

8. Navegar con más seguridad – anónimo y seguro en Internet ... 453

8.1 La víctima de cristal – investigación personal en Internet ... 454
El instrumento estándar: el buscador ... 454
Averiguar direcciones de correo electrónico ... 458
Buscar en los archivos de noticias ... 460
Averiguar la ubicación utilizando la guía telefónica ... 463
8.2 Galletas amargas – las cookies, un riesgo para la seguridad ... 465
Funciones y peligros ... 466
Verificar y borrar las cookies existentes ... 468
Las funciones cookie de los navegadores ... 469
Una cómoda protección con Cookie Pal ... 475
8.3 Anónimo por la Red – navegar sin dejar huellas ... 481
¿Qué información está en juego? ... 481
Haga la prueba: ¡Esto es lo que revela su navegador sobre usted! ... 482
Así se hace: navegar de incógnito por la Red ... 486
Para los que quieran estar muy seguros: el software Anonymizer ... 490

9. Proteger las páginas de inicio contra los hackers 497

9.1 ¿Qué revela sobre usted su propia página web? **499**
Registrar y analizar las páginas web 499
Proteger las páginas web contra los ladrones de información 506
Impedir el uso fraudulento de las imágenes publicadas 510
9.2 Páginas web manipuladas **511**
Proteger las páginas web contra los ataques 512
9.3 Contraseñas, archivos y áreas protegidas **514**
9.4 Posibilidades de ataque sobre servidores web **516**

10. ¿Alternativas seguras? – Linux, windows NT/2000 y Co. 519

10.1 El hermano mayor: Windows NT/2000 ..... **519**
Windows NT/2000 contra Windows 9x/ME 520
El administrador de usuarios en Windows NT/2000 522
10.2 Barato, ¿pero también seguro? – Linux como alternativa **523**
Linux: Unix económico para PCs 524
Hacer segura la instalación de Linux 528

¡Basta de jergas! – el vocabulario del hacker 537

Glosario 557

1. El hacker, ¿ese ser (des)conocido?

1.1 El robo rápido de datos – Anatomía del ataque de un hacker 19
Paso 1: explorar los objetivos potenciales 19
Paso 2: análisis del objetivo de un ataque 24
Paso 3: la elección del método de ataque 40

1.2 El ataque al sistema 41
Sistemas infectados – sabotaje mediante virus informáticos 41
El Gran Hermano te vigila – infiltración de troyanos 42
Puertas traseras – aprovechar los fallos del sistema y los agujeros de seguridad 45
Averiguar contraseñas por la fuerza 47
Control remoto – manipulación de un PC mediante acceso remoto 48
Acceso a sistemas de ficheros desprotegidos 49
Fisgoneo de contraseñas – Password Sniffing 51
Internet, cancha de juego para los hackers 52
Pirateo sin ordenador – Social Hacking 56

1.3 Chicos malos, "script kids" y saboteadores 58
Just for fun – chicos con talento que se aburren 59
Rencor y envidia – compañeros de trabajo envidiosos 60
Hackers clásicos – entusiastas e ideólogos 61
Negocios turbios – espionaje y sabotaje 64
Information Warfare – guerra en la era de la información 65

Para poder batir al enemigo hay que conocerle bien. Atendiendo a este lema, comenzaremos por acercarnos un poco al mito del hacker. Muchos tienen una idea muy imprecisa de lo que es un hacker. Especialmente, la información sensacionalista que publican ciertos medios crea una imagen muy inexacta de amenaza permanente. Frecuentemente, uno se imagina al hacker como un individuo barbudo adicto a la informática, sentado día y noche en oscuras salas de ordenadores, que se alimenta de cantidades industriales de pizza y café, aporrea el

teclado (de ahí el término inglés "hacker") y se mueve como si tal cosa por las redes informáticas de este mundo, buscando siempre el agujero por donde acceder a esos datos secretos tan preciados o a ese servidor protegido de tan difícil acceso.

Ciertamente, esta imagen idealizada ya no se ajusta a la realidad en los tiempos actuales. De acuerdo, sigue habiendo hackers clásicos que actúan simplemente por idealismo y curiosidad. Pero el pirateo informático se está convirtiendo cada vez más en una diversión de masas. Y es que, gracias a Internet, hoy en día cualquiera puede localizar programas y datos que antes sólo estaban accesibles a un círculo reducido y distinguido. Para dedicarse al pirateo, ya no hay que ser un especialista con amplios conocimientos y probada experiencia. Basta con conocer las direcciones apropiadas en la red o saber manejar un buscador para conseguir en un santiamén los datos y programas necesarios.

¿Qué significa realmente hacker?

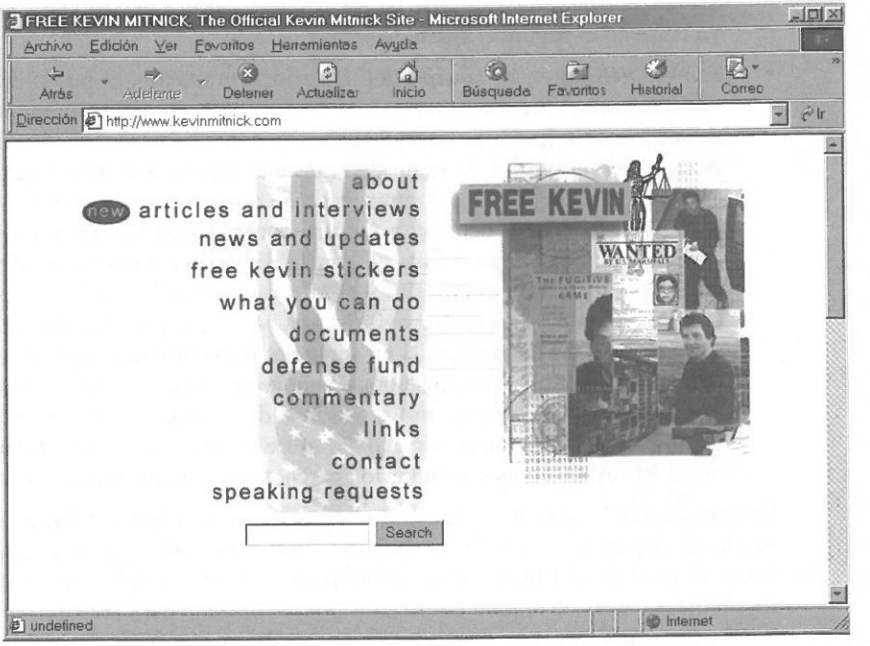
Originalmente, el término "hack" se empleaba para hablar de un truco de programación elegante, o al menos muy inteligente, que permitía obligar al ordenador a hacer ciertas cosas que en realidad, no debía hacer. Aquél que dominara estos trucos debía poseer conocimientos informáticos muy extensos y, por ello, se le llamó hacker. Este término ya existía, incluso cuando dispositivos de entrada como los *mouses* o ratones aún eran impensables y todas las instrucciones se introducían mediante el teclado en forma de comandos. Aquel que tuviera mucha rutina en este aspecto, podía teclear a gran velocidad hasta los comandos más complejos, por lo que literalmente parecía estar machacando el teclado.

Cuando con el tiempo estos astutos trucos de programación fueron utilizados para buscar el acceso ilícito a determinados sistemas, se amplió el término a este ámbito. La expresión "cracker", también utilizada con frecuencia en este contexto, deriva del término "safecracker", el ladrón de cajas fuertes que, como es sabido, también se aplica al acceso ilícito de objetos protegidos. Mientras los hackers son personas más bien constructivas, movidas por un espíritu explorador e inventivo, los crackers se caracterizan, según la definición clásica, por estar en "el lado oscuro del poder". Poseen inclinaciones predominantemente destructivas y la mayoría de las veces, sólo miran por su propio beneficio. El cracker se diferencia del hacker, principalmente, porque en ocasiones destruye intencionadamente los datos ajenos; la destrucción forma parte de sus acciones. Sin embargo, con el tiempo esta dualidad clásica entre hackers y crackers ha ido pasando a un segundo plano, ya que actualmente el panorama está plagado de personas con las motivaciones más dispares. Esto hace imposible mantener la clásica división entre buenos y malos.

INFO

Kevin Mitnick – El hacker más buscado

También el mundo de los hackers tiene sus propios héroes. Uno de los más conocidos en este ámbito, que incluso llegó a alcanzar cierta "gloria" a escala mundial, es Kevin Mitnick. Durante muchos años, amenazó la seguridad de redes informáticas y telefónicas y tuvo fama de ser una persona que podía acceder a todas partes. De hecho, logró una serie de ataques notorios. Incluso llegó a ser incluido en la "Most-Wanted-List" del FBI, la lista de los delincuentes más buscados en los Estados Unidos. Pero acabaron apresándole y tuvo que enfrentarse a varios años de cárcel. Actualmente, está en libertad condicional, pero sigue bajo la prohibición de acercarse a todo tipo de ordenadores o teléfonos durante muchos años. En la dirección http://www.kevinmitnick.com puede acceder a su página oficial, donde encontrará todo tipo de información acerca de su historia.



En http://www.kevinmitnick.com está la página web oficial de Kevin Mitnick, el ídolo de los hackers.

El principio básico del pirateo informático

La finalidad básica del pirateo es rastrear y aprovechar los puntos débiles. Prácticamente cualquier sistema, por muy seguro que sea, tiene su talón de Aquiles. El hacker sólo necesita saber dónde buscarlo. Con la suficiente paciencia, encuentra el punto débil y se hace con el control del sistema, accediendo a

datos confidenciales. En principio, podemos distinguir dos tipos de puntos débiles:

- *Puntos débiles en los sistemas o servidores*: casi cualquier sistema informático tiene agujeros de seguridad. Esto lo ilustra de modo ejemplar el debate sobre la proliferación de puntos débiles en los navegadores de páginas web. También entran en esta categoría la introducción de virus o caballos de Troya, ya que un sistema realmente seguro debería ser inmune a ellos. Los puntos débiles tienen la ventaja de que, cuando se les conoce, casi siempre se les puede sacar provecho sin demasiado esfuerzo. Y gracias a Internet, hoy en día ya no es difícil informarse sobre los agujeros de seguridad. La desventaja de los agujeros de seguridad es que una vez conocidos, suelen ser cerrados rápidamente. En este caso, la aplicación de parches y actualizaciones sólo depende de los administradores de sistemas. Pero esto ya entra en el segundo apartado.
- *Puntos débiles en el equipo del usuario*: con mucho, el punto débil más apreciado es el propio usuario. Los hackers se aprovechan continuamente del desconocimiento, la imprudencia o la comodidad de los usuarios, que desatienden las reglas de seguridad más básicas. Esto se puede aplicar, por ejemplo, al manejo de las contraseñas. Sin duda, resulta comodísimo elegir una contraseña muy cercana a nuestro entorno, que nos resulte difícil de olvidar. Igual de cómodo es apuntarse la contraseña en la parte inferior del teclado o en el cajón del escritorio. Otros puntos débiles del usuario son las configuraciones incorrectas del sistema, en principio, seguras. ¿De qué sirve un sistema hermético, si en segundo plano funciona un servidor FTP con acceso anónimo? O pensemos de nuevo en el administrador de sistemas mencionado más arriba, que quizá sea demasiado ocioso o demasiado incompetente, para mantenerse al día sobre los agujeros de seguridad detectados en sus sistemas e instalar los parches apropiados para cada caso.

En este capítulo, queremos transmitir algunos conocimientos básicos sobre la forma de pensar y actuar de los hackers. Para ello, vamos a mostrar primero cómo se produce el típico ataque de un hacker. A continuación, presentaremos las distintas clases de ataque empleados por los hackers para penetrar en los sistemas. Para finalizar, nos centraremos en los diferentes tipos de hackers y sus motivaciones. Se pretende que esta información le ayude a desarrollar una sensibilidad básica al peligro que representan los hackers para sus ordenadores y datos.

1.1 El robo rápido de datos – anatomía del ataque de un hacker

Cada uno de los ataques que realiza un hacker, presenta un desarrollo bien diferenciado. Esto depende tanto del modo de pensar y actuar del atacante o de su especialización, como de las características del sistema atacado. Sin embargo, el típico ataque hacker posee un esquema básico. Una pauta de pasos que se suceden en un orden determinado.

Paso 1: explorar los objetivos potenciales

El primer paso de un ataque o, para ser más exactos, previo a un ataque, es la exploración exhaustiva de un objetivo potencial. El pirateo no deja de ser un saqueo, pero perpetrado por medios virtuales o electrónicos. A fin de cuentas, un buen saqueador de pisos se toma el trabajo de espiar primero para averiguar cuándo estará vacío el piso, sus posibles entradas, la protección de éstas, si dispone de una buena alarma o a qué distancia está la comisaría más próxima. El buen hacker obra de un modo similar. Primero busca toda la información posible, para lo cual Internet le puede ser de gran ayuda. En muchos casos, partiendo sólo del nombre de una persona o empresa, permite recopilar datos muy completos que finalmente conducen a una dirección y así, a un posible ataque inmediato.

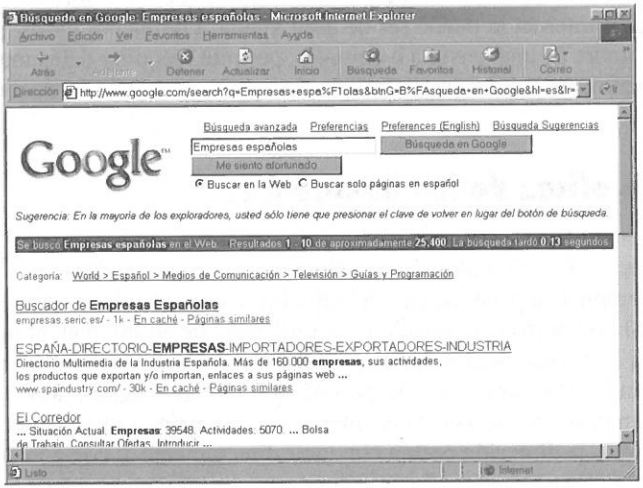
El empleo eficaz de los buscadores

Una herramienta eficaz para indagar en Internet son los buscadores (también para los hackers). Por ejemplo, si se desea obtener información acerca de una determinada empresa o persona, casi siempre basta con introducir su nombre en el buscador. Si esta persona u organización está presente en Internet, el buscador encontrará las correspondientes páginas web. Estas pueden ser muy interesantes por su contenido. Por otra parte, la procedencia de las páginas web también puede ser un importante paso hacia delante. Así, si una empresa gestiona su propio servidor web, la dirección podría conducir directamente al corazón de la red de esa empresa. Con los particulares, pocas veces se tiene esa suerte. Aunque también aquí la búsqueda puede llevar derecho al ordenador de Internet que utiliza esa persona.

La búsqueda de una empresa por Internet puede proporcionar toda una serie de datos interesantes:

- Multitud de información sobre la propia empresa, que puede ser interesante según las intenciones del hacker.

- Datos sobre los empleados de la empresa, que después podrán ser aprovechados para realizar más pesquisas personales, descubrir puntos débiles personales o para ejercer el pirateo social.
- Información sobre las conexiones con otras personas o empresas de servicios, con las que tenga tratos la compañía en cuestión. Son de especial interés las empresas de servicios IT que suministren por ejemplo hardware y software, o que realicen determinados servicios para esa compañía, como hospedaje de webs o acceso a Internet.
- Información sobre la posibilidad de establecer contacto y las ofertas de servicios, que puede ser aprovechada por el hacker para obtener más datos o establecer discretamente contacto con los empleados de la empresa.
- Referencias a sectores especiales en la oferta de Internet, que no están al alcance del público en general y están protegidas por restricciones de acceso.
- Información sobre la estructura IT de la empresa, como por ejemplo el emplazamiento y número de servidores web y otras ofertas del servidor, que podrían ser útiles para un ataque.



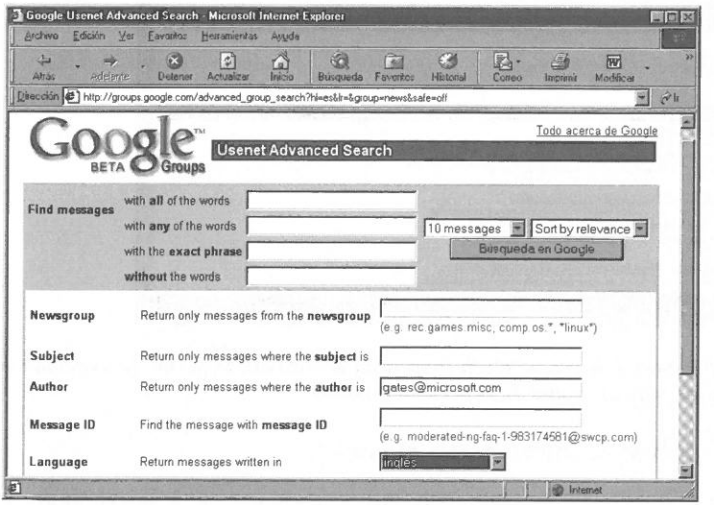
Los buscadores como por ejemplo http://www.google.com pueden proporcionar – de modo gratuito y legal – mucha información valiosa.

En definitiva, las indagaciones sobre una empresa siempre deberían conducir a una o varias direcciones de ordenador de mayor utilidad. Y como mínimo, en todos los casos se podrá averiguar la dirección del servidor web. Aunque no siempre tiene por que ser un ordenador propio de la empresa, como, por ejemplo, cuando el hospedaje de webs ha sido encargado a una empresa de servicios. Como los ordenadores de una empresa por regla general se encuentran en la

misma subred, partiendo de la dirección de ésta se pueden averiguar más ordenadores pertenecientes a la red de esa empresa. Después, en una segunda fase, estas subredes y sus correspondientes ordenadores podrán ser sometidos a un análisis más exhaustivo.

Búsqueda selectiva de personas

Si no se busca una empresa sino una persona, los buscadores también son la primera herramienta a considerar. Por otro lado, existen más posibilidades de indagación que pueden servir de ayuda adicional, especialmente para la búsqueda de personas. Si la persona buscada es activa en Internet y participa en foros de discusión, listas de correo o grupos de noticias, se podrán averiguar más cosas sobre dicha persona. Muchos foros de discusión o listas de correo ofrecen archivos, donde se guardan las contribuciones más antiguas. Por regla general, se puede curiosear en ellas mediante búsqueda de documento entero. Si se busca por el nombre o la dirección de correo electrónico de la persona en cuestión, se pueden consultar los artículos que pudiera haber publicado en el pasado. Incluso los grupos de noticias brindan esta posibilidad. Bajo la dirección http://www.deja.com, encontrarán un archivo que contiene la mayoría de los grupos de noticias y puede ser escudriñado amplia y flexiblemente. Aparte de una búsqueda sencilla por palabras clave, se ofrece también un *Advanced Search* o búsqueda avanzada que permite realizar consultas de búsqueda muy específicas. De esta forma existe la posibilidad de buscar el autor de las contribuciones, indicando el nombre o la dirección de origen de la persona buscada.



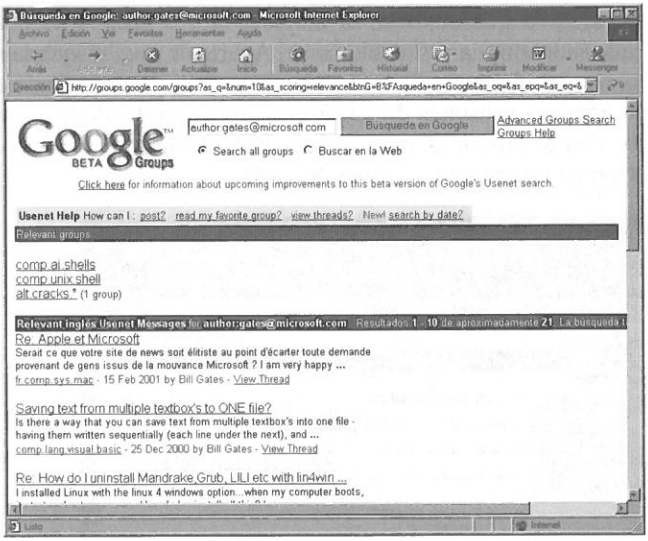
Bajo http://www.deja.com se pueden explorar los archivos de grupos de noticias.

TRUCO

Encontrar contribuciones de noticias de los empleados

También a la hora de investigar una empresa, puede resultar útil una busqueda de este tipo. El *Advanced Search* de Deja.com (perteneciente a Google.com) no sólo permite indicar la dirección de correo electrónico completa de una empresa, sino también parte de la misma. Si por ejemplo se introduce como autor *@microsoft.com*, aparecerán todas las contribuciones de remitentes cuya dirección de correo electrónico contenga microsoft.com. Es decir, con toda probabilidad pertenecerán a empleados de Microsoft.

Como resultado de la exploración, se obtiene una lista de las contribuciones del autor o los autores buscados. Esto permite averiguar por un lado la contribución que publicó la persona en cuestión, cuándo lo hizo y en qué grupo de noticias. Además, las contribuciones también pueden ser extraídas y leídas directamente. Si *Google* o *Deja.com* encuentra a varias personas que se ajusten a lo buscado, se puede pedir la visualización del perfil de artículos enviados de cada posible candidato. Este indicará en qué grupos de noticias publicó contribuciones la persona en cuestión, con lo cual casi siempre se averigua pronto quién es la persona buscada.



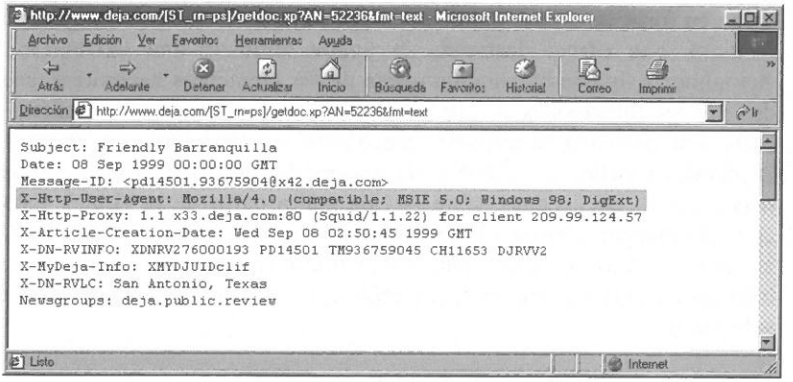
Cuando se hace Advanced Search (búsqueda avanzada), Deja.com proporciona una relación de las contribuciones de la persona buscada.

¿Qué aporta la información online?

Nunca se puede obtener suficiente información acerca de las víctimas. Las propias publicaciones de esa persona siempre son una excelente fuente de informa-

ción. Por un lado, el contenido de una contribución suele ofrecer datos especiales sobre intereses, preferencias, características y costumbres. Éstas pueden ser el punto de partida para futuras indagaciones o para el pirateo social. Así por ejemplo, si a partir de una contribución en un grupo de noticias se averigua el lugar de residencia de una persona, quizá ya baste con echar un vistazo a la guía telefónica correspondiente (o hacer una consulta online) para obtener también la dirección y el número de teléfono. Eso ya nos conduce hasta la misma puerta de la víctima, o nos podemos acercar a ella telefónicamente con algún pretexto.

Pero también bajo el punto de vista técnico, puede resultar muy interesante analizar las contribuciones publicadas por la víctima. Si por ejemplo, una persona se pronuncia en determinados foros sobre hardware o software específicos, se podrán sacar conclusiones sobre su equipamiento informático. Esto a su vez, supone una información importante a la hora de preparar un posible ataque al ordenador de la víctima. Muchas veces, también se puede extraer la información en cuestión de los datos de cabecera de una noticia. *Deja.com* ofrece la posibilidad de ver las contribuciones de noticias en su formato original, inclusive las entradas de cabecera. Muchas veces, éstas contienen datos sobre el software empleado por el autor de una contribución, por ejemplo en la información de cabecera *User-Agent*. A modo de ejemplo, en la siguiente ilustración se puede reconocer, por la cabecera, que el autor de una contribución empleó un PC con Windows 98 como sistema operativo e Internet Explorer 5.0.



Según delata la cabecera, este participante ha elaborado su contribución con Internet Explorer 5 bajo Windows 98.

En el Capítulo 5 nos ocuparemos con más detalle de la búsqueda de personas, con el enfoque de averiguar el máximo de información sobre un atacante y localizarle. También abordaremos más extensamente el empleo de buscadores, archivos y otras ayudas para la averiguación. Pero muchos de esos métodos pueden ser aprovechados igualmente por hackers, para informarse sobre sus víctimas.

Contramedidas

¿Cómo podemos protegernos de ser espiados por agresores a través de los buscadores de Internet? Bien, eso depende ante todo de la cantidad de información que queramos o debamos facilitar sobre nosotros mismos. Hoy en día, estar presente en la Red mejora la imagen de una empresa. La que no ofrece ningún tipo de información y posibilidades de contacto, es tachada rápidamente de anticuada o subdesarrollada. Cosa que no favorece precisamente el negocio. Estar en la Red resulta, por tanto, ineludible. Aunque ahora se plantea la cuestión de qué información hay que facilitar. También en este caso, resulta imprescindible publicar determinados datos específicos como direcciones, información de contacto y datos sobre los empleados o la persona a quién recurrir para determinado tema. Pero se puede evitar enteramente dar información técnica detallada sobre la propia infraestructura, así como el hardware y el software empleados en la red de la empresa. Si aparte de esto, se separan de la red de empresa el servidor web y otras ofertas a las que pueda acceder todo el mundo, encargando su custodia a un proveedor de hospedaje de webs, los hackers lo tendrán más difícil. Si se permite que los empleados participen en foros de debate públicos, habría que adoptar medidas especiales y establecer directrices sobre la información que jamás deberá ser desvelada en esos foros.

Un particular lo tiene mucho más fácil a la hora de proteger sus datos. Para empezar, no es imprescindible que todo el mundo posea una página web o participe en foros de debate públicos. Si por otra parte, no se desea renunciar a las ventajas que ofrece Internet, se puede adquirir una existencia virtual. Actualmente, existe una amplia oferta de los elementos necesarios, como pueden ser las direcciones de correo electrónico y homepages gratuitas. En este caso, si se participa en foros de acceso público sólo habrá que procurar separar la identidad virtual de la real y, de este modo, pretender que un hacker nunca pueda sacar conclusiones sobre la vida real a partir de la virtual. Esto reduce considerablemente las posibilidades de un agresor, ya que, como mucho, podrá atacar elementos virtuales como, por ejemplo, la homepage. Sin duda, esto también puede causar daños, pero por regla general son rápidamente controlables y subsanables.

Paso 2: análisis del objetivo de un ataque

La exploración de los objetivos potenciales ya ha llevado al hacker muy cerca de su víctima. Así que ahora, aparte de un arsenal de información completa, también dispondrá de direcciones. Estas podrán ser reales, por ejemplo para atacar físicamente a un ordenador local. Sin embargo, en la mayoría de los casos lo que interesa son las direcciones de ordenadores, como pueden ser los números o nombres IP de los ordenadores que emplee la víctima, o de los servidores donde

la víctima ofrezca información o servicios. Partiendo de estas direcciones, en una segunda fase el agresor podrá sondear las características técnicas para averiguar posibilidades de ataque concretas.

TRUCO

Servidor

Servidor es la denominación genérica para un ordenador que ofrece determinados servicios en una red. Por ejemplo, si un ordenador de Internet ofrece páginas web para consultas, será denominado como servidor web. En sentido estricto, el término servidor se refiere a la aplicación que ofrece el servicio, es decir, al programa de servicio web. Puesto que normalmente, sobre todo en Internet, se trabaja con servidores especializados, es decir, ordenadores que sólo ejecutan una tarea concreta, el nombre se emplea también como denominación del ordenador global.

Averiguación de servidores y servicios

Para perpetrar una agresión a través de una red como puede ser Internet, se necesitan puntos de ataque concretos. Un ordenador con conexión a Internet no es atacable por sí mismo. Sólo si ofrece determinadas posibilidades de acceso se podrá entrar en él sin permiso. Estas posibilidades de acceso son normalmente los servidores u otros servicios ofrecidos por un ordenador. En la mayoría de los casos, aparte de delatar su propia existencia, dan información sobre el software empleado. Así, se puede averiguar en un servidor web el software que emplea. A partir de ahí, se puede investigar en Internet si para ese software, se conocen agujeros de seguridad o errores de programación que podrían ser aprovechados a la hora de atacar.

Seguimiento de los vínculos de red

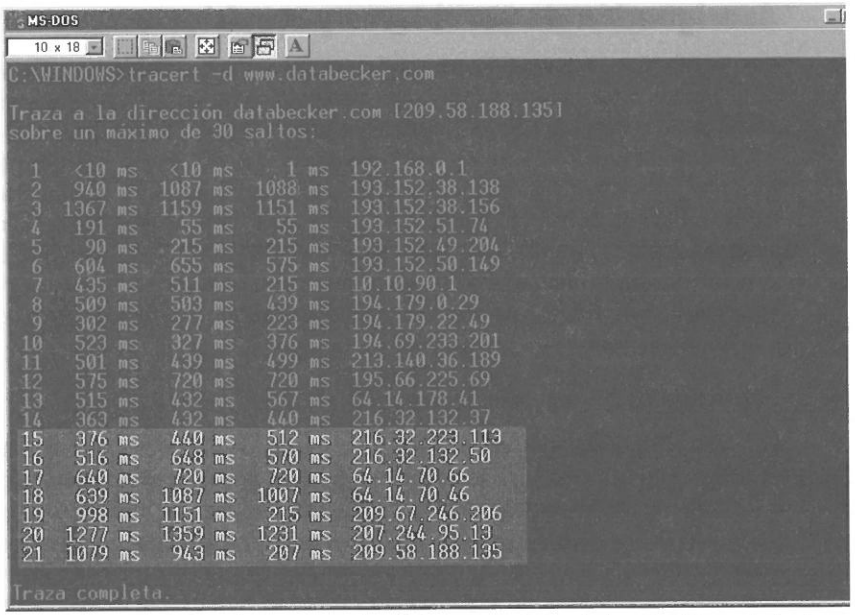
Para atacar el ordenador de un particular, basta con conocer la dirección de ese ordenador. Si por el contrario, lo que interesa es la red de una empresa, primero habrá que espiarla para recopilar la mayor cantidad de información posible. Partiendo de una sola dirección en la red, se pueden averiguar más ordenadores y direcciones. Una forma de hacerlo es analizar la información de las rutas de seguimiento. Una ruta de seguimiento rastrea la ruta exacta de los paquetes de datos TCP/IP en un vínculo, desde el propio ordenador a cualquier otro ordenador en la red. Si, por ejemplo, se hace una ruta de seguimiento a una dirección de ordenador integrado en la red de una empresa, en la mayoría de los casos se obtendrá información valiosa sobre la estructura de la red. Si el tránsito de red se desarrolla, por ejemplo, a través de ordenadores de acceso centrales, que quizá sirvan de puerta de acceso a Internet desde la red de la empresa, estos ordenadores aparecerán en la lista de rutas de seguimiento. Si la red de la empresa se compone de varias subredes y los datos son transferidos de una subred a otra, en la lista de rutas de seguimiento aparecerá al menos una estación para cada subred.

INFO

TCP/IP

Transport Control Protocol/Internet Protocol es el protocolo de red en el que se basa la totalidad de Internet. Regula el intercambio básico de datos entre ordenadores de Internet, en forma de paquetes de datos. Al mismo tiempo, TCP/IP compone una familia de protocolos que abarca todos los protocolos basados en TCP/IP, a saber: HTTP, FTP, POP, SMTP etc. En los siguientes capítulos de este libro nos dedicaremos más a fondo a los diferentes aspectos de TCP/IP y a los miembros de las familias de protocolos del mismo nombre, aplicando sobre todo criterios de seguridad.

En el Capítulo 5 describiremos con mayor detalle cómo manejar la ruta de seguimiento y diversas herramientas disponibles para ello. En el caso más sencillo, para hacer un seguimiento de los vínculos de redes basta el comando de Windows *tracert*.



Resultan especialmente interesantes las últimas estaciones de la ruta de seguimiento, por lo que deberían ser analizadas con más detalle.

Las herramientas especiales como, por ejemplo *NeoTrace*, permiten realizar indagaciones más extensas y cómodas. *NeoTrace* puede representar gráficamente el recorrido de los vínculos de redes. Así, se aprecian aún mejor los ordenadores físicamente cercanos, por lo que se puede deducir que pertenecen a la misma red o red de ordenadores. Además, esta herramienta proporciona prácticamente todos los datos sobre ordenadores conectados al conjunto de redes que se puedan obtener de fuentes oficiales.

NeoTrace permite el análisis gráfico de los conjuntos de redes, además de proporcionar una amplia información.

Sondeo de redes

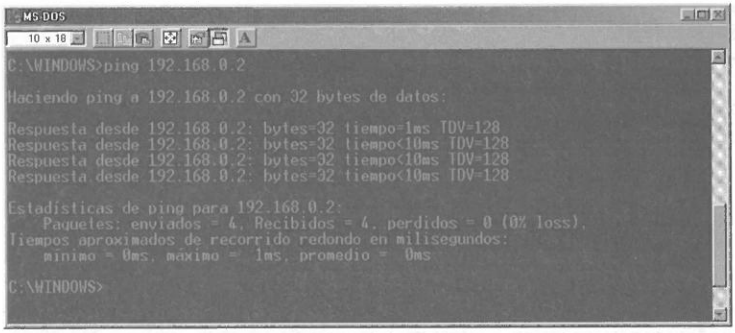
Cuando se conoce uno o varios ordenadores de una red de empresa, surge la pregunta sobre la disposición exacta que presenta esa red, es decir, qué otros ordenadores pertenecen a la misma. Naturalmente, no se puede coger y extraer una lista de los ordenadores, pero se puede hacer un sondeo y ver qué pasa. Utilizando la función *Ping* de TCP/IP, se puede pedir a cualquier ordenador que responda con un breve mensaje de contestación. Si el ordenador lo hace, ya se sabe que existe. De no haber respuesta, puede ser que ese ordenador no exista o que haya sido configurado para no responder a consultas Ping.

INFO

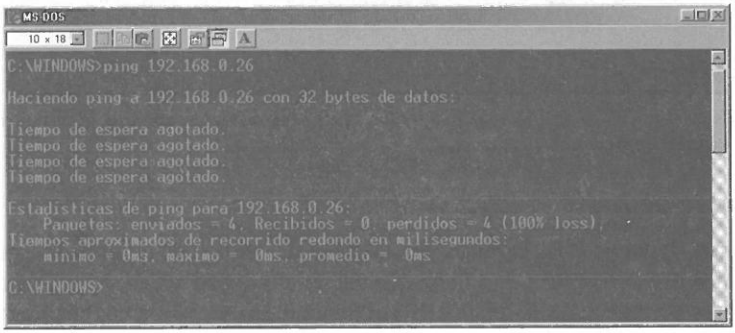
Ping

Packet Internet Groper, Ping, es una función sencilla para comprobar el vínculo de red entre dos ordenadores. Un ordenador envía los requerimientos Ping a otro ordenador y recibe respuesta. Así se sabe que el otro ordenador existe y está en activo. Si, además, se mide el tiempo entre las consultas y la respuesta, se podrá averiguar la velocidad del vínculo.

Ping también está disponible como un sencillo comando dentro de Windows. Si se conoce, por ejemplo, la dirección IP de un ordenador dentro de la red, mediante un Ping se podrá comprobar, en las direcciones adyacentes, si hay más ordenadores conectados a esos números IP. Supongamos que conocemos la dirección *192.168.0.25*. Esto nos permitiría hacer un Ping a las direcciones *192.168.0.24* y *192.168.0.26*, esperar las respuestas y deducir si hay más ordenadores en esa red.



A veces, un Ping da buen resultado y delata a otro ordenador, ...



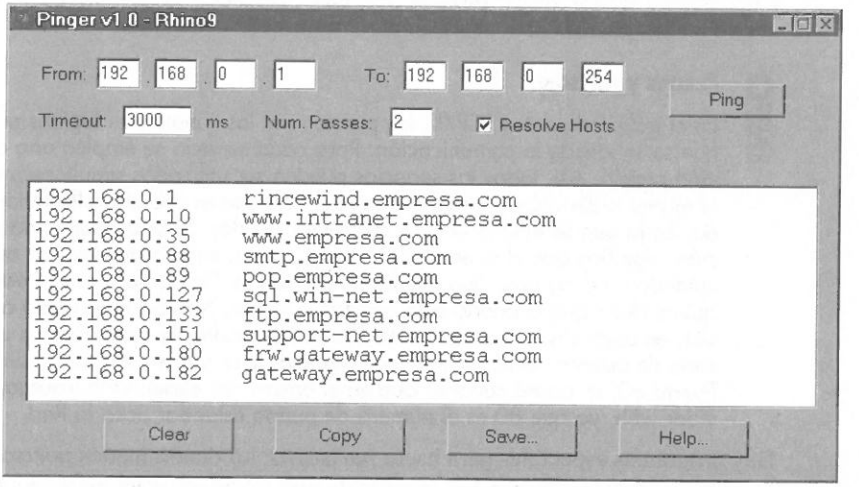
...otras veces se tiene menos suerte y no hay respuesta.

Una subred sencilla puede estar compuesta por hasta 255 direcciones de ordenadores. Con varias subredes en una empresa importante, se incrementa proporcionalmente el número de direcciones potenciales. Contactar manualmente con todas las direcciones mediante Ping, desde luego tiene poco sentido. Para eso hay programas especiales que exploran automáticamente una subred entera, haciendo Ping a todo el intervalo de posibles direcciones de ordenadores y evaluando las respuestas. Una herramienta de este tipo puede ser *Pinger*, que puede ser descargado como freeware bajo la siguiente dirección http://packetstorm.securify.com/groups/rhino9. En estos programas, sólo hay que predefinir el intervalo de direcciones de ordenador que se deseen comprobar (por ejemplo *192.168.0.1* a *192.168.0.254*). Pinger enviará una o varias consultas Ping *(Num. Passes)* a cada una de estas direcciones. Si recibe respuesta dentro del tiempo de espera *(Timeout)* previamente definido, incluirá esa dirección en su lista. Al mismo tiempo, intentará averiguar el nombre IP que corresponda al número IP encontrado. Muchas veces, los nombres también revelan información sobre la función o tarea del ordenador hallado. Los datos recopilados se visualizan en la lista de la ventana de aplicaciones.

INFO

Subredes

Internet se compone de multitud de subredes, es decir, redes parciales menores que abarcan un determinado número de ordenadores. Hay distintas clases de subredes de diferentes tamaños. La organización de las subredes se hace mediante números IP de cuatro partes. Cada uno de los tres primeros bloques de números representa a una subred de diferente tamaño. Se establece una distinción entre las clases A (la mayor) a C (la menor). El cuarto bloque define al ordenador concreto dentro de la subred de clase C.



Pinger permite explorar cómodamente y en poco tiempo redes completas de empresa, para localizar los ordenadores existentes.

Algunos administradores de redes aún se lo ponen más fácil a los hackers, permitiendo el acceso público a la información DNS de su red. Normalmente, estos servidores DNS sólo deberían ser accesibles para ordenadores integrados en la red. Las consultas sobre el DNS desde el exterior ni siquiera deberían estar permitidas. Si pese a todo se permitieran, un agresor podría hacerse prácticamente con un mapa sinóptico de la red de la empresa, donde figuren detalladamente todos los ordenadores existentes.

INFO

Domain Name Service (DNS)

Domain Name Service DNS permite visualizar el número IP de cada nombre IP y viceversa. Es decir, al introducir la dirección www.empresa.com, el DNS averiguará a partir de ésta el número IP del ordenador, que es el que posibilita el acceso. Este servicio de DNS resulta imprescindible. En Internet, por ejemplo, toda una serie de grandes servidores DNS regulan el tráfico de datos. Pero también las redes de empresas disponen frecuentemente de su propio servidor DNS, con el que regulan la administración de los ordenadores de su propia red interna.

Portscans

Una vez descubiertos los ordenadores existentes y sus direcciones, se puede proceder a la exploración de los diferentes ordenadores. Esta irá encaminada a hacerse una idea lo más exacta posible sobre la configuración de red del ordenador, aclarando sobre todo los servicios a través de los que se pueda contactar con el mismo. La comunicación de redes por TCP/IP está subdividida en puertos. Cada servicio de Internet, como por ejemplo WWW, correo electrónico o FTP, emplea uno o varios puertos propios. Utilizando un *portscan*, se pueden averiguar los puertos activables en un determinado ordenador.

INFO

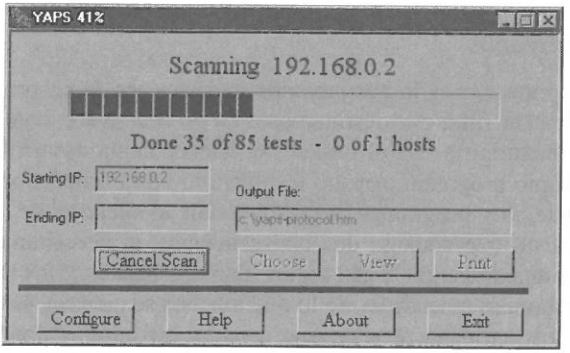
Puertos y portscans

En el tráfico de datos TCP/IP, los puertos son las conexiones lógicas en las que se subdivide la comunicación. Para cada servicio se emplea una conexión propia. Así, todos los servicios pueden ser utilizados simultáneamente en el mismo ordenador y en la misma red. Portscan es una consulta automatizada, en la que se interroga a los diferentes puertos. Si se produce una reacción, significa que el puerto está abierto o bien, en el ordenador se está ejecutando un programa que atiende a ese puerto. De no haber respuesta, quiere decir que el puerto está cerrado o incluso ha sido bloqueado a propósito, en cuyo caso atacarle no tendría posibilidades de éxito. Existen una serie de puertos estándar. Así, por ejemplo, si se obtiene respuesta en el Puerto 80, se podrá suponer que en el ordenador examinado trabaja un servidor web, ya que 80 es el número de puerto estándar para la Red.

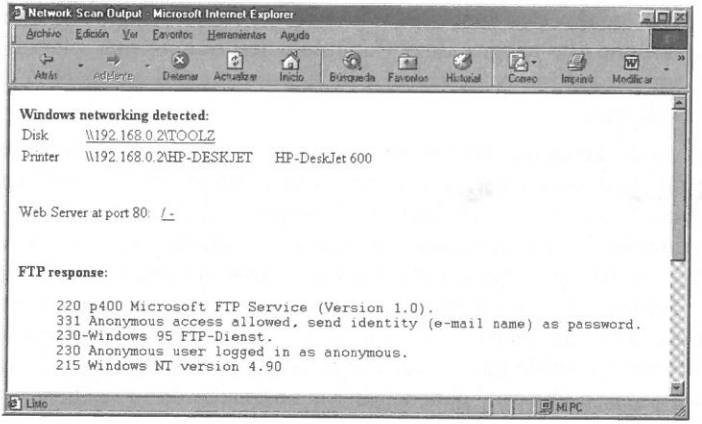
Hay programas especiales para hacer *portscans*, los denominados *portscanners*. Analizan sistemáticamente los puertos de uno o varios de los ordenadores previamente indicados. Permiten tanto comprobar de modo selectivo la existencia de determinados puertos, como realizar sucesivamente una comprobación general de todos los números de puerto que interesen. En el Capítulo 6 presentamos un portscanner de este tipo, YAPS. Este programa no se limita a hacer una comprobación rutinaria de todos los puertos, también verifica la existencia concreta de determinados puntos débiles, producidos muchas veces a raíz de configuraciones incorrectas. Si en lugar de una única dirección de ordenador se indica un intervalo completo, YAPS puede hacer un portscan totalmente automatizado de los ordenadores pertenecientes a toda una subred, confeccionando un inventario exacto del entorno potencial de ataque.

Como resultado, YAPS emite un protocolo del rastreo, donde figuran todos los datos que haya podido averiguar sobre los diferentes ordenadores. Esto incluye todos los puertos donde el ordenador se dejará sonsacar una reacción. Si en el ordenador se ofrecen determinados servicios, YAPS también comprobará enseguida si estos servidores presentan los típicos agujeros de seguridad. Si por ejemplo en el ordenador se explota un servidor FTP, YAPS intentará, automáticamente, iniciar una sesión como usuario anónimo de ese servicio FTP. El de-

sarrollo de este *logon* también queda reflejado en el protocolo. De darse la posibilidad de acceso anónimo, ya se habría detectado un posible punto débil. Habría que comprobar ahora sin falta los derechos de acceso concedidos al usuario anónimo. Normalmente, el acceso debería quedar limitado a la lectura de determinado directorio. Sin embargo, los administradores inexpertos suelen pasar por alto este agujero y no ponen suficientes barreras al usuario anónimo, que se encuentra con considerables derechos de acceso a ficheros. Esto le permite leer ficheros importantes o incluso colar sus propios programas.



YAPS permite escanear los puertos de un ordenador y detectar así posibles ataques.



YAPS proporciona un extenso protocolo de los scans y las comprobaciones que se realicen.

YAPS no fue concebido por su creador para el ataque, sino para testear el propio ordenador o la propia red en busca de puntos débiles. Pero como suele ocurrir con muchos programas de seguridad, el dilema es que también pueden ser empleados por hackers para detectar los puntos débiles de sistemas ajenos. La cuestión siempre está en quién aplica estos programas y cuáles son sus intenciones.

INFO

FTP

File Transfer Protocol, FTP, pertenece a la familia de protocolos TCP/IP y es responsable de la transmisión de ficheros. Es una aplicación cliente-servidor clásica. Esto significa que debe haber un servidor FTP que ponga a disposición los ficheros. Así, empleando un programa FTP (cliente) el usuario puede iniciar una sesión con el servidor y solicitar ficheros. Pero una función *upload* también permite el recorrido inverso, es decir, la transmisión de ficheros desde el cliente al servidor. Tomando como base el programa FTP *WS_FTP*, en el Capítulo 9 nos centraremos también en el manejo de FTP.

La búsqueda de troyanos

Otro aspecto de los portscans es la búsqueda de troyanos, es decir, programas destructivos que el hacker filtra clandestinamente en un ordenador, con la finalidad de espiarle o teledirigirle. En el pasado, el hacker debía desarrollar con mucho trabajo su propio programa troyano e infiltrarlo en el ordenador de sus víctimas. Actualmente, los programas troyanos están al alcance de todo el mundo en Internet. Esto trae consigo dos consecuencias: si necesitamos uno, sólo nos separa de él una descarga. Y aún mejor (para los hackers): los troyanos están hoy en día mucho más extendidos de lo que muchos se piensan. Un número nada desdeñable de usuarios ya tiene en su ordenador troyanos totalmente instalados, que sólo esperan ser activados. Ahora, esos malhechores se infiltran con la misma facilidad que los virus. Si bien es cierto que el uso consciente de los antivirus protege de estas infecciones, la mayoría de los usuarios de Internet no se toman en serio este peligro. En el Capítulo 3 describimos más a fondo el peligro que emana de virus y troyanos. También mostramos cómo protegerse de ellos con eficacia.

Entonces, ¿qué tienen que ver los troyanos con los portscans? Cuando un troyano moderno ha anidado en un ordenador, activa su propio puerto y desde allí acecha noticias de entrada que lo activen y le hagan realizar determinadas funciones. Si un hacker sólo escanea aquellos puertos donde sabe que suelen ocultarse troyanos y recibe una respuesta afirmativa, ya sabe que ese ordenador tiene un troyano. Aunque no sepa gran cosa sobre ese troyano concreto, a través de Internet podrá obtener en cuestión de minutos la información necesaria, o bajarse el software requerido para teledirigir a esos parásitos. Ahora, sólo le queda exclamar "¡Ábrete sésamo!" para acceder al ordenador de su víctima.

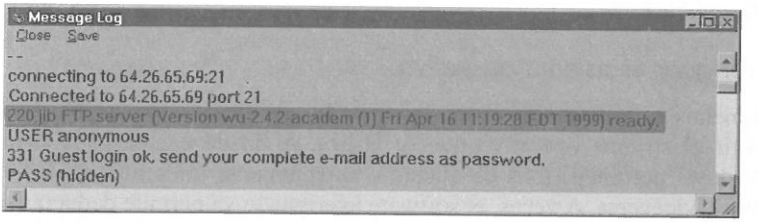
Averiguar el sistema operativo y el software instalado

Una vez obtenida toda la información requerida acerca de los ordenadores disponibles y los servicios que ejecutan, es posible preparar el ataque más a fondo. Como ya hemos descrito al comienzo de este capítulo, hay dos puntos de ataque

esenciales: puntos débiles en el sistema y puntos débiles en el equipo del usuario. Una vez detectados los puntos débiles de un sistema, es fácil sacarles provecho. Pero para eso, hay que conocer más a fondo el sistema. Si se desea aprovechar, por ejemplo, un agujero de seguridad en el software del servidor web, primer hay que saber qué software trabaja en el ordenador que está en el punto de mira. Después, un hacker puede proporcionarse en Internet la información precisa sobre ese software y buscar los agujeros de seguridad conocidos de ese producto. Armado con esos datos, en un siguiente paso podrá probar si los agujeros del sistema atacado ya fueron cerrados o si siguen estando accesibles. Si encuentra un agujero abierto, podrá piratear a la carta, es decir, siguiendo instrucciones ya preparadas y sin necesidad de esforzarse mucho.

Averiguar el software del servidor

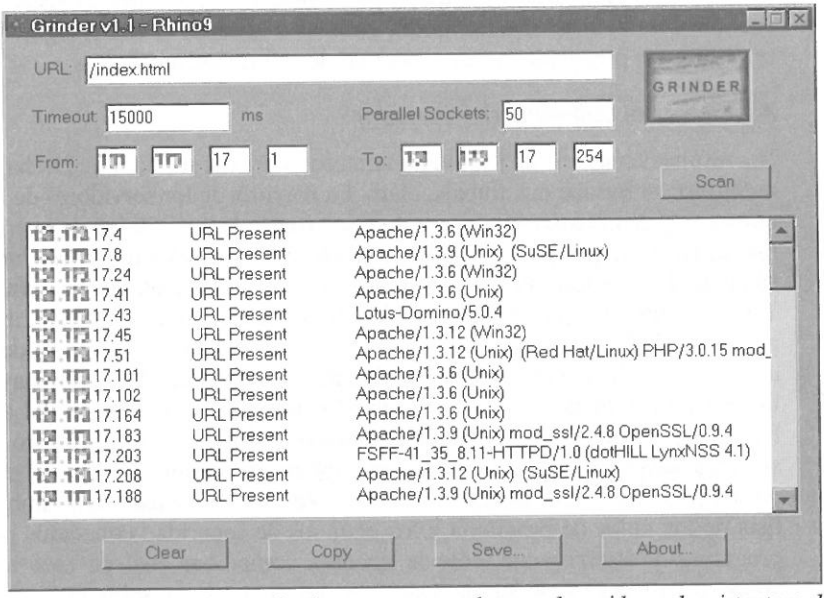
No resulta demasiado difícil averiguar el software del servidor que trabaja en un ordenador, si se sabe que trabaja, claro. La mayoría de los servidores de Internet no se esconden precisamente, con lo que ofrecen la posibilidad de averiguar el tipo de producto y, según el caso, el número de versión. Muchas veces, basta únicamente con emplear el correspondiente programa de cliente para cada servicio. Tomemos por ejemplo el servidor FTP: si usted inicia en él una sesión con un programa FTP como puede ser WS-FTP, recibirá durante el arranque de sesión una amplia serie de mensajes de estado que podrá evaluar. Así, en la mayoría de los casos verá en la ventana de protocolos un mensaje de estado del servidor FTP, entre otros datos, que indica el software utilizado con su número de versión. La siguiente ilustración muestra a modo de ejemplo el popular producto *wu-FTP*. Si un hacker busca ese servidor en Internet, encontrará también una lista de los fallos de programa y los agujeros de seguridad conocidos para ese programa. Posteriormente, sólo le quedará comprobar cuál de esos agujeros sigue abierto en el servidor en cuestión y dirigir su ataque sobre él.



En el protocolo del vínculo FTP encontrarán, entre otros datos, el mensaje de versión del servidor FTP.

Aparte de estos recursos sencillos, también hay herramientas especiales que permiten la búsqueda selectiva de servidores, y con ello, de su tipo y número de versión. Una de ellas es por ejemplo *Grinder*, que permite explorar subredes enteras para buscar servidores web. Este programa es del mismo tipo que *Pinger*, ya

explicado anteriormente. Puede obtenerse como freeware en la misma dirección. La tarea de Grinder es escanear todos los ordenadores dentro de un intervalo de direcciones de ordenador previamente indicado, para buscar servidores web en funcionamiento. Al tener los servidores web el puerto estándar 80, esto resulta bastante sencillo. Si Grinder encuentra lo que buscaba, además, intentará averiguar el software que utiliza el servidor web inclusive su número de versión. A veces, los datos incluyen hasta información sobre el sistema operativo empleado, o permiten sacar conclusiones sobre el mismo.



Grinder permite explorar subredes enteras, para buscar el servidor web existente y el software empleado.

Averiguar el sistema operativo

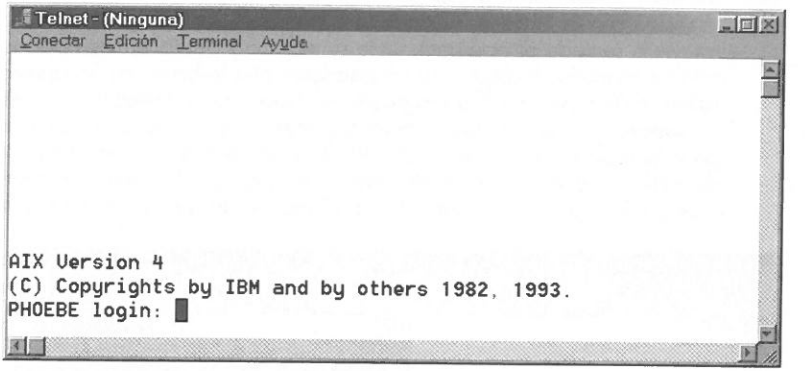
Al menos tan interesante como descubrir los programas empleados, resulta descubrir el sistema operativo que se utiliza. A fin de cuentas, los sistemas de Windows permiten tipos de ataque completamente diferentes de los sistemas Unix y viceversa. A veces, el software averiguado ya permite deducir el sistema operativo sobre el que se basa. Y es que algunos productos de servidor sólo están disponibles para sistemas operativos muy concretos. A veces, el propio software del servidor delata si se trata de la versión para Unix o para Windows. Pero aparte de esto, también existen posibilidades de identificar el sistema operativo. En los ordenadores Unix, muchas veces basta con un simple Telnet, es decir, montar un vínculo de teletrabajo con el ordenador en cuestión. Windows, por

ejemplo, incluye un programa Telnet. Para arrancarlo, hay que seleccionar *Inicio/Ejecutar* e introducir en el menú de ejecución el comando *telnet*. Ahora, sólo quedaría introducir la dirección del ordenador y establecer el vínculo.

INFO

Unix

Unix es un tipo de sistema operativo muy diferente a Windows, diseñado, en origen, para una utilización multiusuario y bajo entornos de red. Las raíces de Unix son mucho más antiguas que las de Windows. No existe "un sólo" Unix, sino una amplia gama de variedades de Unix, lo que se denomina como derivados. Para los PCs, Linux es uno de estos derivados Unix que goza cada vez de mayor popularidad y aceptación. Hablaremos con más detalle de él en el Capítulo 10, donde examinaremos hasta qué punto sirve como alternativa a Windows.



Mediante Telnet, se puede consultar en ordenadores UNIX el sistema operativo que emplean.

Ya al iniciar el comando Telnet, la mayoría de ordenadores comunican la versión de Unix que emplean. Lo más decisivo: el mensaje suele llegar antes de iniciar la sesión. Es decir, no hace falta disponer de identificación de usuario ni contraseña para el ordenador. Una vez obtenida la información deseada, basta con interrumpir el arranque de sesión. En el ejemplo de la ilustración anterior, el inicio de sesión tuvo lugar en un ordenador con sistema operativo *AIX* en *Versión 4*. Esto es una variante especial de Unix con IBM. Disponiendo de esta información, un agresor se puede dedicar a buscar los puntos débiles del producto.

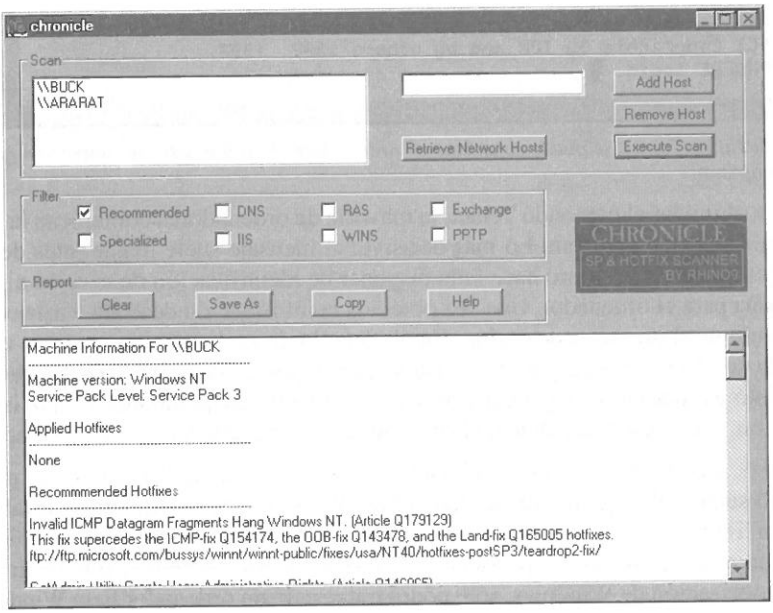
Este sencillo método no funciona en los ordenadores de Windows, ya que estos no suelen ofrecer ningún acceso Telnet. Por lo tanto, ni siquiera se establecería un Telnet con un ordenador de este tipo. Pero aquí existen otras posibilidades, como por ejemplo, un portscan con YAPS. Si éste encuentra referencias a una autorización de Windows, sólo podrá tratarse de un ordenador bajo Windows, ya que esto es un indicador típico. Además, también para esta tarea se pueden conseguir programas especiales. Como ***Chronicle***, otro producto del creador de

Pinger y *Grinder*, que está especializado en ordenadores Windows NT. Puede explorar automáticamente toda una subred en busca de ordenadores con ese sistema operativo. Por cada ordenador que encuentre, averigua, además, los Service Packs que tenga instalados. Así denomina Microsoft los ficheros de actualización y reparación, destinados a cerrar los agujeros de seguridad que se detecten. Si se sabe qué Service Packs lleva instalados un ordenador y cuales no, se sabrá naturalmente los agujeros de seguridad que ya fueron cerrados y los que siguen abiertos. Además, chronicle advierte expresamente sobre los agujeros de seguridad y los problemas que tengan las distintas máquinas, por no haber sido instalados los Service Packs correspondientes.

INFO

Telnet

Telnet es un servicio especial perteneciente a la familia TCP/IP. Permite iniciar la sesión con un ordenador a través de una red y teledirigirlo, como si se estuviera sentado directamente ante su teclado y pantalla. Los vínculos Telnet sólo se pueden establecer con ordenadores que trabajen en un sistema operativo multiusuario real, como puede ser Unix. Los ordenadores de Windows no soportan Telnet de origen. Pero disponen de un programa Telnet sencillo para teletrabajar desde el PC de Windows en otro ordenador. Hay productos de software especiales para PCs con Windows, que también permiten este teletrabajo. Pero por razones de seguridad, se desaconsejan estas soluciones.

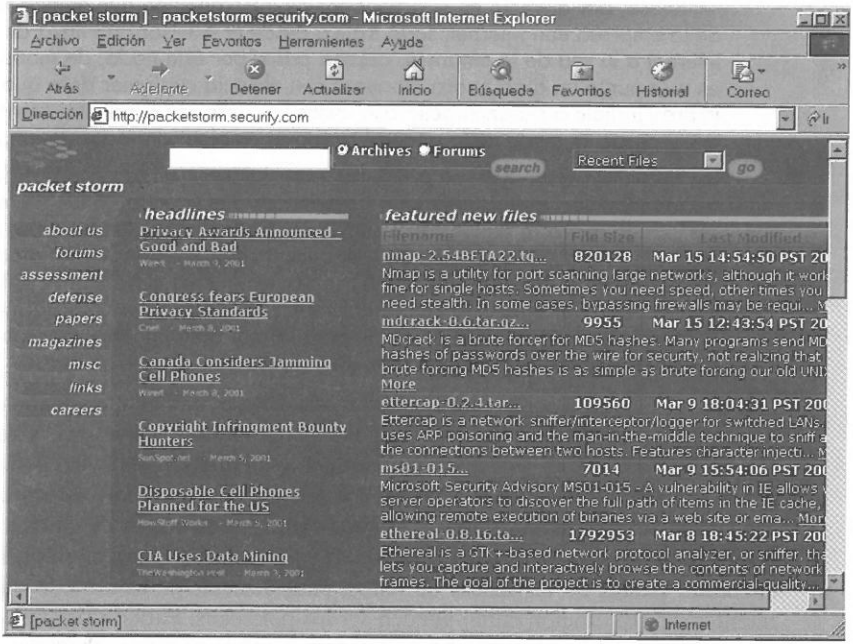


Con chronicle se puede analizar el estado de los ordenadores NT de Windows y detectar sus puntos débiles.

INFO

Los programas de Rhino9

En este apartado hemos presentado tres programas de Rhino9: *Pinger*, *Grinder* y *chronicle*. Las tres herramientas tienen una cosa en común: sirven para analizar redes u ordenadores integrados en una red. Ahora bien, si los está empleando un administrador de red que quiere analizar su red y eliminar peligros potenciales, o los está aprovechando un hacker para obtener información sobre redes ajenas y preparar un ataque, es algo que los programas no pueden saber. En este punto, quisiéramos advertir expresamente que sólo hemos presentado estos programas, para demostrar el proceder básico de los hackers a la hora de obtener información. Si usted quiere emplearlos para comprobar las debilidades de sus propios ordenadores o redes, podrá descargar los ficheros gratis bajo la siguiente dirección: http://packetstorm.securify.com/groups/rhino9. En la misma página web encontrará, también, multitud de información, consejos y programas recientes sobre cómo proteger los sistemas informáticos de los hackers. Pero, por otra parte, esta oferta en la web refleja claramente la problemática fundamental de que, prácticamente cualquier programa e información útil para protegerse de los hackers, también puede servirles de herramienta para lanzar sus ataques.



Bajo http://packetstorm.securify.com encontrará multitud de informaciones y programas de protección.

Contramedidas

¿Es posible protegerse contra el espionaje del propio ordenador o entorno de red? Con un poco de esfuerzo, desde luego que sí. La mayor parte de información que puede conseguir un hacker consiste en datos, que fuera del ordenador o la red no son asunto de nadie. Así que se podría configurar la red de tal manera, que simplemente no desvele esta información superflua pero delatora. La mejor solución para esto sería un *firewall* o *cortafuegos*. Para los usuarios particulares que sólo se conectan con su PC a Internet cuando lo necesitan, una solución profesional de tipo firewall es demasiado complicada y excesivamente cara. Pero dirigidos a este sector, existen los firewalls personales. En el Capítulo 4, trataremos más en detalle el empleo de las soluciones firewall. También presentaremos dos productos para el sector de usuarios particulares de Internet mediante conexión por módem o adaptador RDSI.

INFO

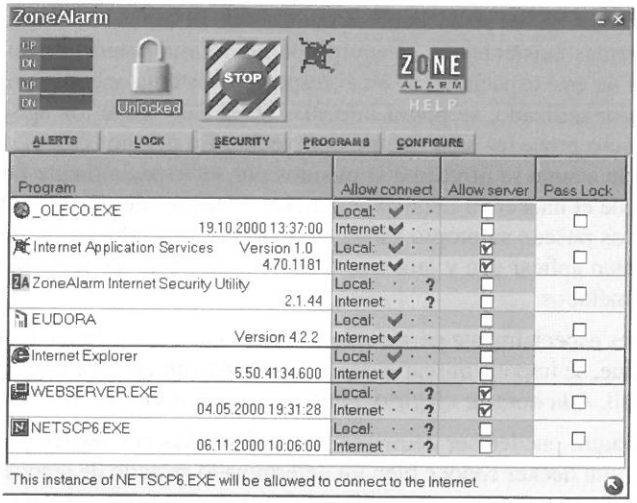
Firewalls y firewalls personales

Se denomina como firewall a un componente de red que filtra y controla el tráfico de datos en un determinado nodo. Se instala en un sitio tácticamente ventajoso, por ejemplo en el ordenador de interconexión que enlaza la red de la empresa con Internet. Todo tráfico desde el exterior que fluya de Internet a la red de la empresa, deberá pasar por este nodo, de manera que en este punto un filtro podrá bloquear con eficacia cualquier dato que no sea imprescindible o parezca peligroso. Estos firewalls son productos complicados y caros, que por regla general se suelen emplear en redes de empresa.

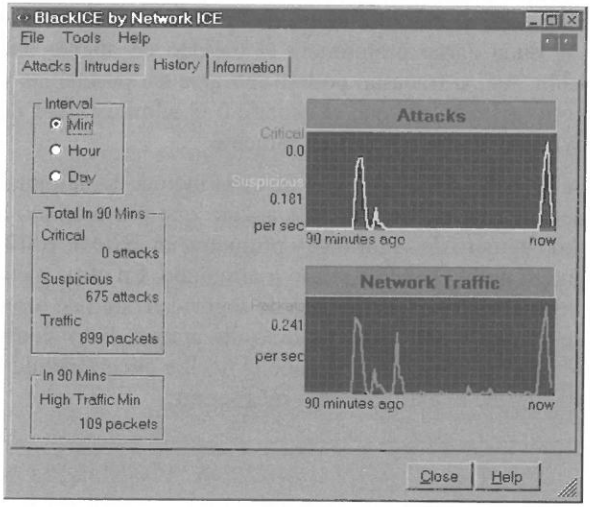
Los firewalls personales son productos especiales concebidos para ordenadores individuales, que asumen una función muy similar a la de los "verdaderos". En la mayoría de los casos suelen ser bastante más fáciles de manejar para el usuario, pero ofrecen una seguridad comparable. De este modo, cuando usted lo necesite podrá interrumpir totalmente el tráfico de datos con Internet, permitir el acceso sólo a determinados programas o escudriñar el contenido de los paquetes de datos para buscar determinado concepto en clave y bloquear los paquetes correspondientes.

Los firewalls suelen ser sistemas pasivos, es decir, evitan ataques y abusos pero no se defienden de ellos. En caso de violación de las configuraciones y reglas de filtraje del firewall, se producirá, como mucho, un mensaje de aviso o una entrada en el protocolo. En este aspecto, los ***Intrusion Detection Systems (IDS)*** especiales avanzan un paso más. También controlan el tráfico de datos y vigilan las incidencias especiales y los intentos de acceso ilícito. Pero, además, intentan encontrar pautas en las masas de datos, para detectar de este modo ataques o intentos de exploración como pueden ser los portscans. Para un firewall clásico, un portscan sólo es una serie de paquetes de datos que serán rechazados o aceptados en función de la configuración. Por el contrario, un programa IDS reconocerá en estos paquetes de datos la pauta típica de un portscan y podrá reaccionar en consecuencia. Las reacciones pueden incluir por un lado un aviso inmediato

al usuario y por el otro, la averiguación del autor que lanzó el ataque. La finalidad de un IDS es detectar los ataques lo antes posible, para poder acabar con las fechorías del agresor y evitar que se produzcan daños. En el Capítulo 6 presentamos con BlackICE un producto de este tipo para PCs individuales.



Los firewalls personales como ZoneAlarm pueden proteger de modo eficaz a los PCs individuales.



Los programas IDS como BlackICE vigilan el tráfico en la red y buscan las pautas características de un ataque.

Paso 3: la elección del método de ataque

Una vez concluida la fase de recopilación de la información, comienza la planificación del ataque. En primer lugar, corresponde identificar los puntos en los que es posible atacar. Como ya hemos dicho, Internet puede suponer una valiosa ayuda, ya que es donde se encuentran multitud de información sobre los sistemas y programas existentes en el equipo de la víctima potencial. Aunque el propio agresor no esté especializado en el respectivo sistema operativo o el software de servidor utilizado, se podrá informar en la Red sobre los agujeros de seguridad y cómo proceder para sacarles provecho. En muchos casos, determinados puntos de ataque se ofrecen a sí mismos por ser especialmente fáciles de aplicar, o porque el hacker ya tiene experiencia en ataques de este tipo. Muchos hackers expertos poseen su propio estilo, un modo de proceder de eficacia probada que intentan aplicar una y otra vez. Sólo cuando ya no les salga bien, buscarán nuevos métodos.

Si un sistema es especialmente permeable y ofrece una amplia gama de posibles puntos de ataque, se impone buscar el mejor punto de entrada. Por decirlo así, el punto más débil. A la hora de elegirlo, pueden intervenir varios criterios.

- También aquí, pueden ser decisivas las preferencias personales y la experiencia. Si un hacker conoce bien un determinado método de ataque y ya lo ha empleado varias veces con éxito, casi siempre lo preferirá a un método que le sea totalmente desconocido.
- A los hackers profesionales les gusta proceder con la máxima discreción posible. Procuran dejar el menor número de huellas, o mejor ninguna. Por eso, en caso de duda darán preferencia al método de ataque que llame menos la atención. Así, si fracasan podrán retirarse sin problemas y seguir probando con otro método, sin que el usuario o el administrador del sistema atacado haya sido alertado innecesariamente.
- Finalmente, las probabilidades de éxito de cada método tienen una importancia fundamental. Existen métodos de ataque que por ejemplo aprovechan determinado agujero de seguridad y prometen un éxito al 100%, siempre que ese agujero no haya sido cerrado o arreglado. En otros métodos, el éxito no sólo depende del propio agujero de seguridad, sino de otros factores que sólo se darán durante el transcurso del ataque. Esto siempre trae consigo grandes imprevistos, de modo que el hacker generalmente preferirá el método con el que el éxito parezca más seguro.

1.2 El ataque al sistema

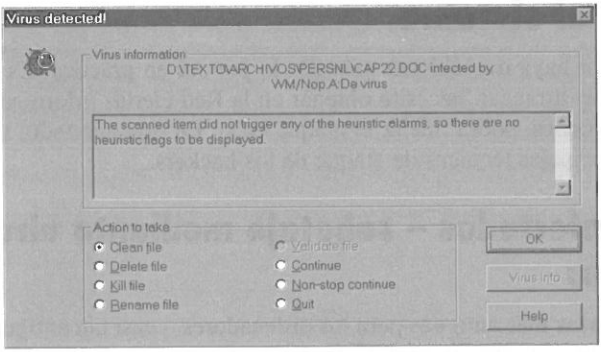
Cuando el agresor haya decidido su método, lo pondrá en práctica. Es posible que antes de poder arrancar, necesite obtener en la Red ciertas informaciones o programas. Y entonces, podrá iniciar el ataque en sí. En este apartado, vamos a presentar las principales técnicas de ataque de los hackers.

Sistemas infectados – sabotaje mediante virus informáticos

Una de las amenazas más antiguas para los ordenadores – casi tan antigua como ellos mismos – son los virus informáticos. En un tiempo mínimo pueden infiltrarse dentro de sistemas informáticos en red e infectarlos. En el ordenador infectado pueden ejecutar prácticamente todas las acciones que quieran, causando por ejemplo la pérdida de datos. En realidad, los virus informáticos no son la herramienta típica del hacker. Pero en manos de un saboteador que sólo pretenda hacer daño, pueden ser armas poderosas. Atacar con virus informáticos resulta comparativamente sencillo, ya que el único requisito que exige es emplazar de algún modo un fichero infectado en un ordenador. Del resto, se encarga el virus.

Los antiguos programadores de virus gozaban de una consideración casi tan mítica como los hackers clásicos. Pero eso ha cambiado de raíz. Hoy en día, para programar un virus ya no hace falta ser un experto. En Internet hay kits de virus completos que permiten confeccionarse su propio virus informático, sin necesidad de poseer unos conocimientos previos especiales. Por ejemplo, para un acto de sabotaje sobre la red de una empresa se puede crear un nuevo virus especial, cuya firma no sea reconocida por el software antivirus instalado. Si el saboteador es empleado de la empresa con acceso interno, podrá comprobar antes si realmente los detectores de virus no detectan al intruso. Así, el parásito digital se puede propagar sin impedimentos. Hasta que no sea evidente su efecto destructivo, no podrá ser detectado ni combatido.

El éxito de un ataque mediante virus depende – igual que en los virus biológicos – de la fase de incubación. Si un virus tiene un período de incubación largo y tras la infección permanece mucho tiempo inactivo o se limita a propagarse sin causar aún daños, podrá extenderse ampliamente por una red antes de que sea detectado y combatido. Si por el contrario, un virus se activa inmediatamente después de la infección y comienza enseguida su labor destructiva, casi siempre suele ser detectado pronto y combatido antes de que el parásito haya encontrado su modo de propagación óptimo.



Los buenos antivirus detectan los virus informáticos y los pueden eliminar inmediatamente.

Contramedida: protección contra los virus informáticos

Las medidas de protección contra los virus informáticos son de sobra conocidas. Sólo ayudan unas medidas preventivas fundamentales y el empleo de programas antivirus eficaces y, sobre todo, siempre actualizados. Estas medidas no sólo deben servir para protegerse de un sabotaje, sino también para evitar la amenaza general de los virus informáticos que, como es sabido, no sólo se emplean de forma selectiva sino también pueden propagarse de modo totalmente arbitrario. Todo esto es una verdad de cajón. Aun así, muchos usuarios no la tienen en cuenta, ya sea por desconocimiento o comodidad. Para una red de empresa, se recomienda también emplear un eficaz detector de virus de red acompañado de un firewall. Así se puede evitar de modo centralizado una infección desde el exterior. Y, además, los empleados ya no estarán obligados a evitar por sus propios medios las infecciones por virus. Para poder armarse también contra los virus totalmente nuevos que el escáner de virus aún desconozca, se recomienda emplear métodos de búsqueda heurísticos. Estos son procedimientos que pueden detectar a los virus por un código de programa típico, en lugar de basarse en la firma. La mayoría de los antivirus ya disponen de estas funciones, aunque frecuentemente no se empleen porque pueden prolongar la comprobación. En el Capítulo 3 nos dedicaremos a fondo a las medidas de protección contra virus informáticos.

El Gran Hermano te vigila – infiltración de troyanos

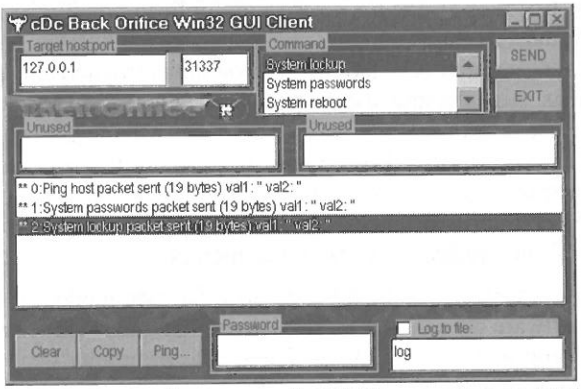
Los troyanos o caballos de Troya no son del todo diferentes a los virus, por lo que muchas veces suelen ser metidos en el mismo lote. Pero la gran diferencia

entre los virus y los troyanos es que los virus se multiplican por sí mismos propagándose cada vez más, mientras que los troyanos no suelen hacerlo. Más bien ocurre que los hackers instalan selectivamente programas troyanos en el ordenador de sus víctimas. Actualmente, esto tampoco es ya del todo correcto, por haber causado Internet la propagación masiva de los troyanos, que no difiere mucho de una infección por virus. Los componentes de un troyano suelen ser ocultados en un software libre de toda sospecha, que es ofrecido después para descarga gratuita. Si el usuario instala ese software se activará automáticamente el troyano, que podrá ser teledirigido a través de Internet.

Un troyano es un programa que se disfraza de otro. De este modo, un agresor podría sustituir el software de acceso a un servicio online que usted tenga en su ordenador, por un programa propio. Desde fuera, este programa tiene casi el mismo aspecto que el original. Pero en realidad, hace cosas completamente diferentes. Por ejemplo, podría preguntar como siempre por su identificación de usuario y su clave, para establecer después una conexión online. Pero en lugar de conectarle a usted con su servicio online, el programa llama al ordenador del hacker y le transfiere los datos de acceso. Como después establecerá la conexión habitual con el servicio online, usted no advertirá nada y el malhechor podrá utilizar su acceso sin ser molestado. Al menos, hasta que usted reciba la siguiente factura del servicio online.

Otra trampa similar es la instalación de un programa de espionaje en el ordenador de la víctima. Éste registra clandestinamente todas las acciones y entradas del usuario, al igual que el tecleo de contraseñas y otros datos delicados. Los registros son grabados en un fichero y evaluados posteriormente por el malhechor. Si el ordenador dispone de una conexión online, el programa *Log* podrá transmitir los datos directamente al agresor a través de la Red. Estos programas de hecho pueden ser detectados, pero los agresores se aprovechan de que, generalmente, nadie los busca.

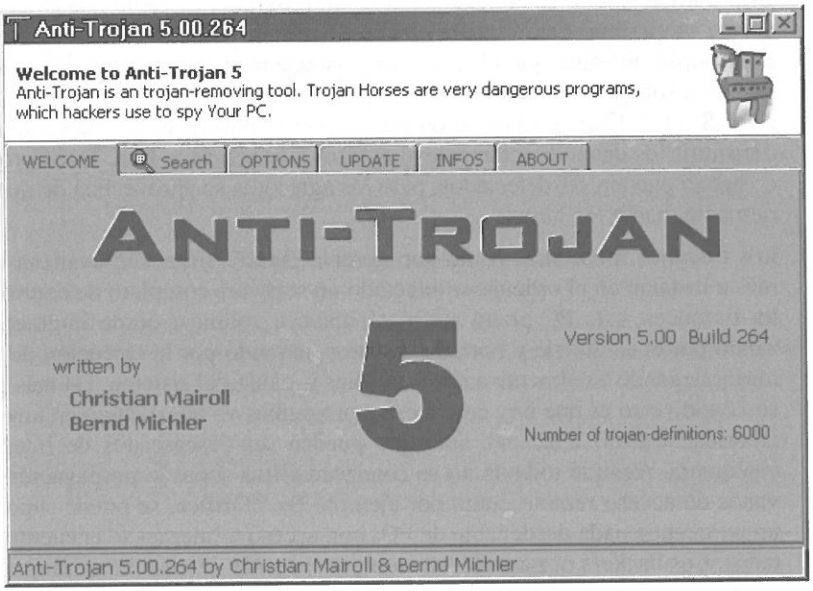
Los troyanos modernos, como por ejemplo *BackOrifice*, aún avanzan un paso más e instalan en el ordenador infectado un software completo de control remoto. Entonces, este PC podrá ser manipulado a voluntad desde Internet, empezando por el espionaje y borrado de datos, pasando por la ejecución de programas y llegando finalmente a desencadenar la caída del sistema. Lo más peligroso de todo esto es que hoy en día estos programas ya no se crean en una fase de laborioso trabajo artesanal, sino que pueden ser descargados de Internet por cualquiera. Aunque todavía no se conozcan cifras sobre la propagación de troyanos de acceso remoto como por ejemplo BackOrifice, se puede suponer que un porcentaje nada desdeñable de PCs con acceso a Internet se encuentran afectados. Los hackers ocasionales ni siquiera necesitan ya instalar el programa troyano. Basta con que rastreen los troyanos existentes mediante portscan y después los activen.



Los troyanos modernos como BackOrifice permiten un total control remoto de otros PCs a través de Internet.

Contramedidas: protección contra troyanos

También en cuestión de medidas protectoras, se suelen equiparar frecuentemente los troyanos con los virus. Esto tiene la ventaja de que los programas antivirus corrientes se ocupan por igual de este tipo de parásitos.



Para combatir a los troyanos, las herramientas especiales son más eficaces que los programas antivirus convencionales.

De modo que con un software antivirus actualizado, también se suele tener una buena protección contra los troyanos. Por consiguiente, en cuestión de protección contra troyanos rige lo mismo que ya se ha dicho sobre las medidas para evitar los virus informáticos. Pero aparte de esto, ahora se dispone de software especial para detectar y eliminar los troyanos, que tiene más en cuenta cómo funcionan estos programas, por lo que también alcanza mejores cuotas de éxito. Dedicaremos el Capítulo 3 al tema de los troyanos y especialmente, a cómo combatirlos con las herramientas adecuadas.

Puertas traseras – aprovechar los fallos del sistema y los agujeros de seguridad

Un método muy popular por su sencillez es el de aprovechar los agujeros de seguridad ya conocidos de sistemas operativos y programas. Prácticamente todos los productos de software tienen agujeros de este tipo. Los programas han alcanzado hoy en día tal complejidad, que ya nadie es capaz de tener en cuenta todas las posibilidades. No digamos ya, de probarlas. Un hacker con la experiencia necesaria y buen olfato siempre encontrará algún punto, donde los programadores hayan sido poco cuidadosos. Desgraciadamente, muchos hackers publican en Internet los agujeros de seguridad detectados, junto con instrucciones para aprovecharlos. Así quedan al alcance de todo el mundo y hasta hackers ocasionales sin demasiada experiencia ni conocimientos pueden sacar provecho de esos agujeros.

Contramedidas: cerrar inmediatamente los agujeros de seguridad

La protección contra los agujeros de seguridad forma parte de las medidas de seguridad más costosas. No es algo que se pueda resolver de un plumazo, más bien es un proceso de información constante. Y es que lo más importante en los agujeros de seguridad es descubrirlos cuanto antes. Por desgracia, precisamente en lo que respecta a los usuarios particulares, los fabricantes de software no aplican una buena política de información. En este tema, los legisladores deberían imponer disposiciones mucho más claras con respecto a la responsabilidad sobre el producto. Por el contrario, en los productos de software en el ámbito de empresa, hace tiempo que se considera de buen tono que el fabricante advierta a sus clientes inmediatamente sobre los posibles riesgos para la seguridad. Hasta que esto ocurra también en el campo de los clientes particulares, sólo nos queda la iniciativa de informarnos a través de los diferentes medios. Resulta de gran utilidad la lectura regular de revistas del sector, ya que suelen dedicar gran atención a los informes de errores y a las advertencias. Algo más actualizado está Internet, que es donde se difunden en primer lugar los informes de errores. Aunque la búsqueda de las páginas web y los grupos de noticias sale algo más cara.

En las páginas web como por ejemplo http://winfiles.cnet.com/bugs se puede obtener información sobre los fallos y los agujeros que ya se conozcan.

Parches y Bugfixes

Cuando se han detectado errores, los fabricantes de software suelen reaccionar con pequeñas reparaciones (denominadas como *bugfixes* o *parches*). Normalmente, estos ficheros son accesibles desde Internet. Muchas veces, el fabricante los envía si se le solicita, o los reparte en los CDs de las revistas de informática. Desgraciadamente, aparte de la reparación en sí, estos ficheros reparadores suelen contener más errores. Antes de instalar uno de estos ficheros de reparación, piense bien si lo necesita realmente. Utilice el fichero sólo, si:

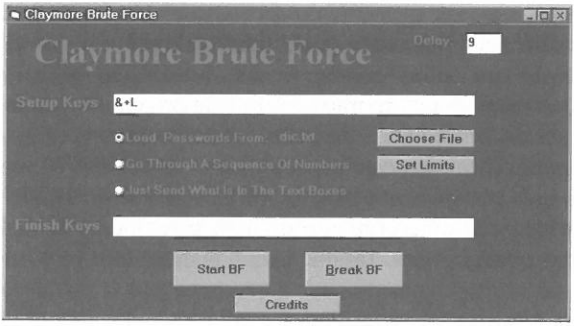
- resuelve un problema que le afecte a usted realmente,
- proporciona una función adicional que usted quiera utilizar de verdad,
- tapa un agujero de seguridad que suponga un peligro personal para usted o sus datos,
- se basa en un software que usted necesita sin falta.

Le desaconsejamos categóricamente la instalación de todos los parches disponibles, sólo porque estén ahí.

Averiguar contraseñas por la fuerza

El objetivo de la mayor parte de los ataques hacker son las contraseñas, ya que protegen el acceso a los sistemas y datos buscados. Sólo es posible eludir la petición de contraseña si existe el correspondiente agujero de seguridad y éste es conocido. De lo contrario, hay que apropiarse de la contraseña por las buenas o por las malas. Para eso hay varios métodos. Se puede espiar la contraseña empleando recursos técnicos, o averiguarla recurriendo a la investigación social. Si todo esto falla, sólo quedará ya la fuerza bruta. Este concepto, al que en ambientes hacker se alude con el término inglés *Brute Force*, es el último recurso para hacerse con la contraseña. Por eso, este método suele ser el último en emplearse, ya que resulta muy costoso comparado con los otros. Como contrapartida, su cuota de éxito suele ser alarmantemente alta.

En los ataques por fuerza bruta, los hackers emplean programas que averiguan la contraseña a base de probar. Estos disponen por ejemplo de diccionarios y prueban sucesivamente todos los términos de los mismos como contraseña, hasta haber encontrado la palabra clave buscada o haber agotado la lista de palabras. Desgraciadamente, casi siempre se suele cumplir la primera alternativa. Como muchos de estos programas pueden ser obtenidos libremente en Internet, hoy en día cualquiera puede bajarse el correspondiente programa con extensos diccionarios y emplearlo. Por eso, resulta imprescindible disponer de una protección eficaz contra los ataques por fuerza bruta.



Con programas que están al alcance de todos, como por ejemplo Claymore, cualquiera puede averiguar contraseñas mediante ataques por fuerza bruta.

Contramedidas: protección contra ataques a la fuerza

En realidad, protegerse de los ataques de contraseña a la fuerza es lo más sencillo. Elija contraseñas útiles y seguras. Como los hackers suelen emplear para sus ataques listas de palabras y diccionarios, usted debería tener una contraseña que

no figure en estas listas. Para eso, lo mejor es utilizar una combinación cualquiera de letras, números y símbolos especiales. Estas palabras clave son imposibles de desencriptar, incluso con ataques por fuerza bruta. En las redes de empresa, el administrador del sistema debería ocuparse de que los usuarios empleen contraseñas seguras. Eso se consigue por un lado mediante la formación adecuada de los usuarios. Por el otro, empleando sistemas que sólo permitan contraseñas seguras o comprueben periódicamente la seguridad de las mismas.

Otro medio para evitar los ataques por fuerza bruta es un procedimiento de inicio de sesión seguro. Los sistemas fiables por ejemplo sólo permiten tres intentos sucesivos de iniciar una sesión con una contraseña incorrecta. Después, la entrada queda bloqueada o como mínimo, deberá transcurrir cierto período de pausa. Igual que ocurre con el código secreto en los cajeros automáticos o el PIN de los teléfonos móviles. Si se han introducido tres códigos incorrectos, hay que salirse antes de poder hacer un nuevo intento. Los ataques automáticos por fuerza bruta tienen poco éxito con estas medidas de seguridad.

Control remoto – manipulación de un PC mediante acceso remoto

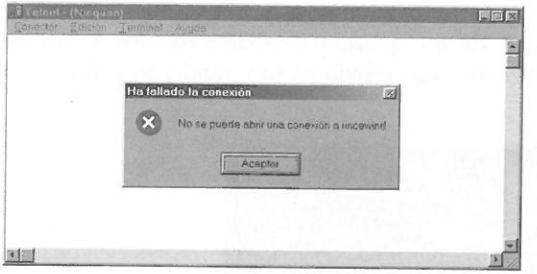
El objetivo final de muchos hackers es hacerse con el control total de un ordenador remoto, para perpetrar definitivamente un ataque. Así tendrán las mismas posibilidades y los mismos derechos que un usuario que esté sentado físicamente ante la pantalla. Por eso, los métodos de acceso remoto gozan de especial popularidad entre los hackers. Si existen posibilidades de este tipo y cuáles son, depende enteramente del ordenador atacado. Se puede decir que los ordenadores Unix llevan este acceso remoto incorporado, ya que de origen ofrecen la posibilidad de iniciar una sesión desde otro ordenador, mediante Telnet por ejemplo, y trabajar como un usuario local. En este aspecto, los ordenadores Windows son algo más seguros ya que, por citar un ejemplo, los PCs Windows 9x/ME no vienen equipados de origen con ningún medio de acceso remoto. Para establecer este acceso, hay varias posibilidades. También aquí, la más próxima es averiguar los nombres de los usuarios y las contraseñas que permiten el acceso. Aunque también hay siempre agujeros de seguridad y configuraciones incorrectas, que permiten un acceso remoto no autorizado.

Contramedida: evitar el acceso remoto no autorizado

La problemática específica del acceso remoto es que se trata de una función que en realidad se desea poner a disposición del usuario. Pero al mismo tiempo, esta función encierra un enorme potencial de riesgo, por lo que convendría preguntarse siempre si el acceso remoto es realmente imprescindible y conveniente. De no serlo, habría que desactivarlo sin falta para evitar un ataque por este flanco.

Si se dispone de la posibilidad de acceso remoto, debería vigilarse sobre todo que se empleen contraseñas seguras. Además, habría que estudiar si se oculta a los usuarios con acceso remoto determinadas funciones del sistema y datos de naturaleza especialmente crítica. Por ejemplo, se podría configurar el ordenador Unix de tal manera, que un usuario con los derechos de acceso de un administrador de sistema no se pueda conectar mediante acceso remoto. Así se lograría que, aunque un hacker haya conseguido entrar por acceso remoto, no pueda realizar cambios importantes en la configuración del sistema.

Un riesgo de seguridad considerable en los sistemas Linux, de creciente popularidad también entre los usuarios particulares, puede ser que generalmente en la instalación estándar se activa el acceso por Telnet. Muchos usuarios no lo saben, por lo que desconocen totalmente ese boquete potencial en la seguridad. En el Capítulo 11 trataremos, entre otros temas, el sistema operativo Linux, mostrando cómo se puede proteger una instalación estándar de Linux desde todos los flancos.



Si no son imprescindibles, lo mejor sería desactivar totalmente las posibilidades de acceso remoto.

Acceso a sistemas de ficheros desprotegidos

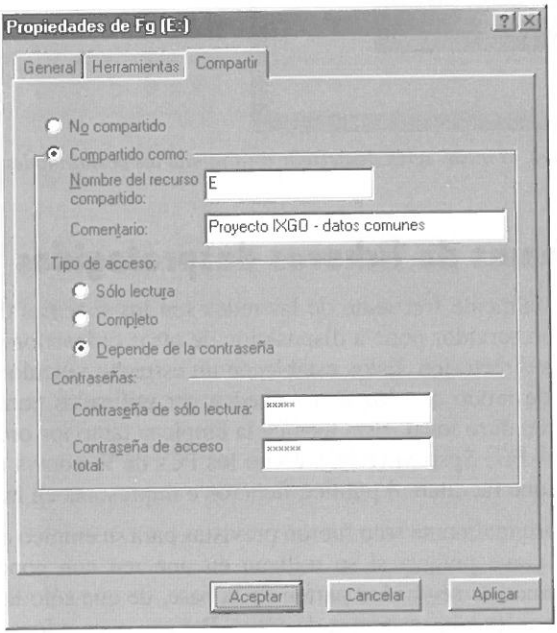
Una utilización especialmente frecuente de las redes son los sistemas de datos repartidos. Es decir, un servidor pone a disposición de otros ordenadores determinadas partes de sus directorios. Estos establecen un estrecho vínculo con los directorios remotos, de modo que los datos pueden ser utilizados como si se encontraran en un disco duro local. Esta técnica la emplean tanto los ordenadores Unix con ***Network File System*** (NFS), como los PCs de Windows con uso compartido de datos, que facilitan al público ficheros e impresoras en las redes.

Como estas técnicas originalmente sólo fueron previstas para su empleo en redes locales, suponen un grave peligro si se utilizan en una red con conexión a Internet. Los mecanismos de seguridad parten de la base, de que sólo los usuarios locales pueden acceder a los sistemas de datos. Por eso, van enfocados primordialmente a evitar que se cometan errores por descuido, más que a servir de

protección eficaz contra los ataques de hackers externos. Por esta razón, dejan a los agresores muchos agujeros de seguridad por los que se pueden colar. Y una vez logrado el acceso, aparte de los documentos confidenciales también quedan al descubierto los ficheros de contraseñas y configuraciones, con lo que a veces ya no hay obstáculos para hacerse con el control total del sistema.

Contramedida: proteger los datos desprotegidos

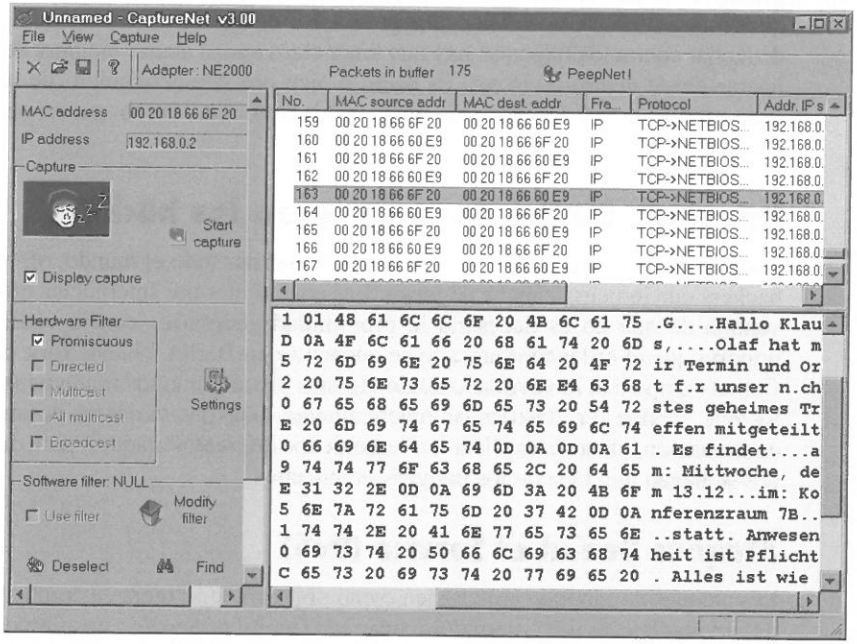
La mejor protección contra este tipo de ataques consiste, siempre que sea posible, en no emplear los sistemas de datos repartidos si la red está vinculada a Internet a través de una vía de acceso. En cualquier caso, la vía de acceso debería disponer de una protección eficaz por firewall. Además, habría que emplear de modo consecuente las medidas de protección aplicables al uso compartido de datos en la red. El uso compartido de datos en Windows, por ejemplo, permite proteger por password las carpetas de red desprotegidas. Sólo quien conozca la contraseña podrá acceder a los ficheros. Sin embargo, muchos usuarios se deciden equivocadamente por la variante cómoda y liberan los ficheros sin protegerlos mediante password. En el Capítulo 6 detallaremos a fondo la problemática del uso compartido de datos bajo Windows, mostrando, además, cómo emplearlo con eficacia.



Si se comparten datos en la Red, habría que hacerlo correctamente y con seguridad.

Fisgoneo de contraseñas – Password Sniffing

El fisgoneo de contraseñas es un método que permite averiguar contraseñas, incluso las que fueran elegidas con la máxima seguridad. En la mayoría de redes, cualquier ordenador conectado puede interceptar todos los paquetes de datos que transiten de un determinado ordenador de la red a otro, sin necesidad de participar directamente en la comunicación. Con programas fisgones se pueden espiar todas las transmisiones de datos de los ordenadores adyacentes (en técnicas de red). En las conexiones para las que se exige un logon con nombre de usuario y contraseña, estos datos críticos siempre se transmiten como paquete de datos al comienzo del enlace. Los programas de espionaje registran estos paquetes y los graban en su fichero histórico. Si un programa de estos es ejecutado durante algunas horas en una red con bastante utilización, el hacker podrá averiguar una gran cantidad de datos de acceso. Pero no sólo se pueden espiar así contraseñas, sino también muchos otros tipos de información confidencial. En el Capítulo 6 explicamos cómo funcionan los programas fisgones y presentamos uno de ellos.



Un fisgón de paquetes permite espiar en texto claro el intercambio de datos en la red entre ordendores adyacentes.

INFO

Un hacker de 20 años roba números de tarjetas de crédito

Bajo http://www.heise.de/newsticker/data/pab-13.07.00-000/ se puede consultar el caso típico de un hacker caído en la criminalidad. Habla de un hacker que, entre otras hazañas, entró en los ordenadores de la NASA. Tras haber logrado infiltrarse instaló un fisgón de paquetes, entre otros programas, para interceptar información confidencial. Así se hizo con miles de datos de acceso e información sobre tarjetas de crédito que fueron hallados en el momento de su detención. El hacker aprovechó los datos de las tarjetas de crédito para adquirir artículos de gran valor.

Contramedida: dejar fuera a los fisgones

El peligro de los ataques por fisgoneo de contraseñas está en que los usuarios prácticamente no adviertan nada. Para ellos, el arranque de sesión transcurre con toda normalidad. Por eso resulta tan difícil protegerse contra ellos. La mejor solución sería ejecutar el inicio de sesión codificado. Pero hoy en día, la versión actual de los protocolos TCP/IP no proporciona esta posibilidad. Es de suponer que los próximos desarrollos de los protocolos de Internet la incluyan. A la hora de luchar contra los fisgones, hay que tener claro que el ataque siempre debe realizarse desde dentro de la red. Es decir, o bien procede de alguien "de la casa", o de un hacker del exterior que antes ha de conseguir como sea un acceso al ordenador integrado en la red.

Internet, cancha de juego para los hackers

Especialmente Internet, con sus comunicaciones por todo el mundo, ofrece a los hackers una inmensa cancha de juego. Las conexiones por Internet les ofrecen la ventaja de que no es necesaria la proximidad geográfica con la víctima. No importa que el ordenador atacado se encuentre en Berlín, Nueva York o Tokio. Con el tiempo han ido evolucionando algunos procedimientos fundamentales, en los que pueden ser clasificadas prácticamente todas las variantes de ataque. A continuación, vamos a explicar brevemente los diferentes ataques, para que ustedes se hagan una idea de los peligros potenciales.

Ataques Denial of Service (DoS)

Los ataques de sabotaje puro tienen como objetivo dejar fuera de combate determinados servicios de un servidor o una red (*Denial of Service*, en español: denegación del servicio). Un modo altamente eficaz para lograrlo es inundar de consultas a ese servicio, que en algún momento llegará a verse desbordado sólo con recibir esas consultas. Un ejemplo clásico de ataque por "Denial of Service" serían las bombas de e-mails descritas en el Capítulo 7, con las que se puede atacar un servidor de correo. Pero también se puede colapsar un servidor web, creando

un programa que en un tiempo mínimo genere constantemente nuevas peticiones HTTP. Una variante del "Denial of Service" que se ha puesto de moda últimamente, son los ataques ICMP. Aquí se emplean comandos especiales de ***Internet Control Message Protocols*** (ICMP), que controlan el flujo de datos a través de Internet. Así por ejemplo, un atacante podría enviar a un servidor un mensaje ICMP, que mande al ordenador no remitir más paquetes de datos a ciertos sectores de la red o incluso a toda la red. Los servidores quedan fuera de combate con un solo comando. Es posible protegerse de este tipo de ataques, empleando un firewall que debe ser instalado de modo que filtre todos los comandos ICMP.

INFO

Guerra en la Red

Febrero de 2000 entrará en la historia de Internet como el mes de los ataques DoS. Durante ese mes, un gran número de importantes sitios web, entre ellos páginas mundialmente conocidas como CNN, eBay, Yahoo y Amazon, fueron víctimas de ataques DoS bien organizados que pusieron fuera de servicio a los servidores de las empresas, en algunos casos durante horas. El suceso trajo consigo pérdidas económicas considerables, sobre todo para empresas como Yahoo, eBay o Amazon, cuyos ingresos proceden exclusivamente de Internet. Aparentemente no hubo motivo para esos ataques. Los expertos suponen que las causas pudieron ser demostraciones de poder de grupos de hackers. Un efecto secundario interesante: las acciones de las empresas afectadas que cotizaban en bolsa, bajaron ostentosamente tras conocerse los ataques. Para quien quiera más detalles sobre esta historia, en el archivo de noticias de ZDnet hay numerosos artículos. Un buen punto de entrada es: http://www.zdnet.com/zdnn/headlinearchive/

En principio, los ataques "Denial of Service" son medidas de puro sabotaje. El agresor no puede esperar conseguir acceso a un ordenador o datos, ni obtener otro tipo de ganancia. Frecuentemente, este tipo de ataques se emplean para vengarse, perjudicar a la competencia, llamar la atención o para utilizarlos como arma en una guerra de información (vea al respecto también el último apartado de este capítulo). Sin embargo, el pasado más reciente ha demostrado que los ataques DOS sí pueden traer beneficios. De esta forma, los ataques a importantes ofertas de Internet como *Yahoo!* o *eBay* depararon un fuerte tirón a la cotización de las empresas de la competencia. Tras finalizar los ataques se recuperaron rápidamente las cotizaciones. ¿Quizá todo fue obra de un hacker con un depósito de acciones?

Ataques DoS repartidos

Una variante especial de los ataques "Denial of Service" son los ataques repartidos, denominados también como ***Distributed Denial of Service*** o abreviadamente *dDoS*. Se caracterizan porque la consulta no procede sólo de un ordenador, sino es enviada simultáneamente desde muchos ordenadores de Internet.

Así, se consigue de forma más rápida el efecto de sobrecarga deseado. Además, siempre resulta más difícil defenderse de un ataque lanzado desde varios flancos. Realmente perverso. Muchas veces, los propietarios de los ordenadores implicados en el ataque ni siquiera sospechan su suerte. Los hackers instalan clandestinamente troyanos en ordenadores ajenos, que después pueden configurar y arrancar con un comando a través de Internet. Un solo hacker puede reunir fácilmente gran número de ordenadores con los que lanzar un eficaz ataque repartido. Él mismo no tiene necesidad de participar con su ordenador, por lo que no corre peligro de ser descubierto como causante.

Contramedidas: evitar los ataques DoS

Por regla general, resulta difícil protegerse de los ataques "Denial of Service". Esto resulta lógico, teniendo en cuenta que esta clase de acosos también pueden darse en la vida real no informática. Suponga que alguien llamara a todos los establecimientos de la ciudad donde sirvan pizzas a domicilio y pidiera a cada uno que llevara diez pizzas a su dirección. Ya puede imaginar lo pronto que estaría desbordado, mientras se enzarzaba con 20 o 30 repartidores de pizza por el pago de la factura. Pero, ¿cómo habría podido protegerse contra eso? El problema fundamental de los ataques DoS es su detección. A fin de cuentas, la sobrecarga de un servidor puede deberse a multitud de causas. Cuando la NASA puso regularmente en la Red imágenes e información actualizada sobre la misión a Marte, la expectación suscitada también puso a los servidores web constantemente al borde del colapso (¡algunas veces, hasta lo rozaron!). Y en este caso, no se trató de un ataque malévolo.

Actualmente se está trabajando sin tregua en el desarrollo de programas para la detección, lo más precoz posible, de los ataques "Denial of Service". En un ataque DoS sencillo, aún se podría descubrir al autor y bloquear los datos de su dirección. Pero los ataques DoS repartidos serían más difíciles de evitar, ya que parten simultáneamente de muchos ordenadores. ¿Cómo distinguir quién está implicado en el ataque y quién quiere entrar sólo en una página web? Aquí, a los ingenieros de sistemas aún les queda por estrujarse un poco más la cabeza.

Ataques mediante manipulación de IP

Una variante de ataque especialmente peligrosa es la manipulación de paquetes IP. Aparte de su propio contenido, un paquete IP contiene una amplia gama de información necesaria para transmitir los datos desde el remitente hasta el destinatario. Algunos de estos datos se dejan manipular de tal modo, que los hackers hasta pueden neutralizar con ellos las funciones protectoras de algunos firewalls.

Con *IP-Spoofing* el hacker falsifica la dirección de origen en un paquete IP. Si quiere atacar un ordenador de la Red que esté protegido por un firewall, asigna-

rá a sus paquetes de datos la dirección de origen perteneciente a un ordenador integrado en la misma red que el ordenador objetivo. Si los paquetes de datos se topan con un firewall, este comprobará su dirección de origen. Al ser esta la de un ordenador que está detrás del firewall, los paquetes serán considerados como seguros y admitidos. Sin embargo, hoy en día la técnica de IP-Spoofing es ya ampliamente conocida y la mayoría de soluciones firewall actualizadas emplean otras técnicas para diferenciar los paquetes de datos internos de los externos.

Otro punto de ataque en los paquetes IP es la *Source Route Option*. Normalmente, los paquetes IP se buscan ellos mismos su camino a través de Internet, para lo cual eligen el más favorable. Pero también existe la posibilidad de indicar con exactitud en la Source Route Option de cada paquete, el camino que éste debe seguir. De este modo, en los sistemas mal protegidos se puede eludir el firewall guiando a los paquetes de datos directamente hasta el ordenador objetivo.

Los ataques con paquetes IP no proporcionan a los hackers el acceso a datos confidenciales. Pero casi siempre son el primer paso para entrar en un ordenador ajeno. Y muchas veces, son un recurso muy útil para penetrar en una red protegida por firewall. Además, suponen un enorme peligro de sabotaje. En principio, basta con que un único paquete IP alcance su meta para ejecutar un comando destructivo en el ordenador objetivo.

Contramedidas: evitar la manipulación IP

El mejor recurso contra los paquetes IP falsificados es una solución firewall eficaz, que conozca los trucos de los hackers y se pueda proteger contra ellos. Por eso, es de vital importancia mantenerse al día constantemente, informarse sobre las nuevas técnicas y, si fuera necesario, actualizar el firewall o adaptar la configuración. Generalmente, los usuarios particulares no tienen que temer a una manipulación IP. Ésta requiere de algunos conocimientos específicos y sólo suele ser empleada por expertos que prefieren atacar objetivos importantes.

Interceptación y secuestro de conexiones abiertas

La mayor parte de redes están basadas en la tecnología Ethernet, donde todos los ordenadores conectados a la Red pueden acceder a todos los paquetes de datos que circulen por la misma. Puesto que las conexiones TCP/IP trabajan sin codificar, un hacker que posea el software adecuado podría rastrear en la red el tráfico de datos entre el ordenador *A* y el ordenador *B*, desde un tercer ordenador *C*. Tras haber observado una conexión durante un rato podría ir incluso más lejos, asumiendo él mismo la conexión. Para eso, generaría paquetes de datos cuya apariencia haga pensar que proceden del ordenador *A* y los mandaría al ordenador *B*.

Para burlar los mecanismos de sincronización de TCP/IP, basta con que envíen los paquetes de datos, siempre, antes que el ordenador *A*. El ordenador *B* recibirá en primer lugar los paquetes de datos infiltrados y desechará como antiguos los paquetes que le lleguen después desde el ordenador *A*. Esto prácticamente echa de la conexión al usuario del ordenador *A*. Él pensará que se ha producido una avería en la red, al haber dejado de reaccionar repentinamente el ordenador *B*. Pero en realidad, ocurre sencillamente que el hacker se ha hecho desde el ordenador *C* con la conexión del usuario. Si éste ya había iniciado la sesión con su contraseña, el hacker "heredará" sus derechos de acceso a ficheros y servicios.

Contramedidas: proteger las conexiones contra los secuestradores

La interceptación y el secuestro aprovechan las debilidades intrínsecas de TCP/IP. En principio, funcionan con todo tipo de conexiones. Pero resultan de especial interés las conexiones de acceso remoto como puede ser Telnet. Aquí, los usuarios poco pueden hacer para protegerse, aunque estos ataques suelen ser muy costosos y requieren profundos conocimientos de TCP/IP. Si bien, actualmente, ya hay programas en Internet que ofrecen las funciones correspondientes con una superficie apetitosa. Una protección realmente eficaz sólo la pueden prestar los administradores de sistemas, tomando las medidas de prevención y vigilancia adecuadas. El secuestro de las conexiones TCP/IP suele presentar algunos síntomas típicos, que pueden ser detectados y clasificados por un administrador de sistemas con experiencia. Como esta clase de ataques se suelen perpetrar dentro de una red, a veces no resulta difícil dar con el causante.

Pirateo sin ordenador – Social Hacking

Un método que les gusta emplear, sobre todo, a los hackers experimentados, es el *Social Engineering* (en español: algo así como investigación social), denominado también *Social Hacking*. Aquí, el hacker se ocupa exhaustivamente del entorno social de la víctima, para averiguar informaciones importantes como pueden ser las contraseñas. La experiencia ha demostrado que la gente suele emplear como contraseña términos relacionados con su vida cotidiana, para poder recordarla más fácilmente. Algunos ejemplos corrientes:

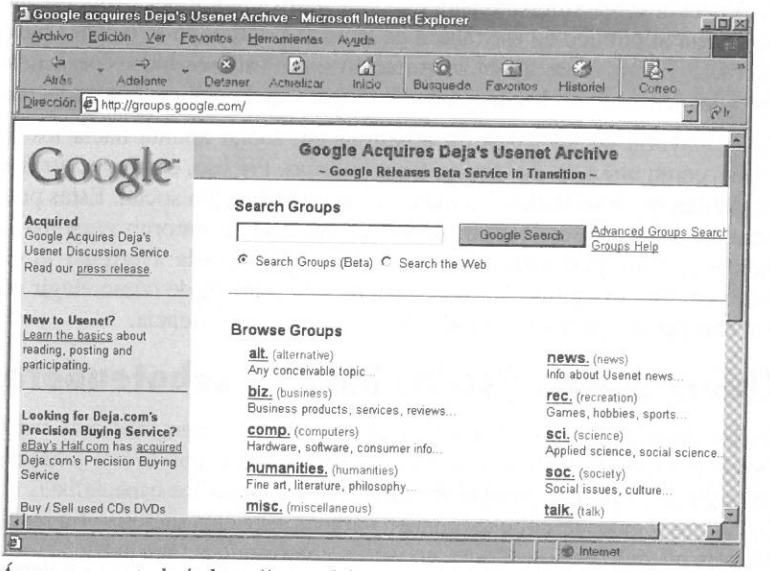
- el nombre de esposas, novias, hijos, mascotas,
- los colores, grupos musicales, canciones, coches, guisos favoritos, o
- datos como cumpleaños, matrículas de automóviles, números de teléfono, etc.

Si un hacker consigue hacerse con el máximo de información sobre intereses, preferencias y costumbres de su víctima, podría confeccionarse una lista con posibles contraseñas, que podría probar cada vez que la víctima del ataque acceda como usuario.

¿Cómo se apropian los hackers de información personal?

Las fuentes de información para los hackers curiosos son muy variadas. En el caso más sencillo, se comienza por la guía de teléfonos. Con un poco de atrevimiento personal, los hackers pueden observarle a usted para enterarse de dónde y cómo vive, con quién, si tiene mascotas y el coche que conduce. Quizá se acerquen con cualquier pretexto a sus vecinos, para sonsacarles todos los detalles que puedan. Quién esté interesado en los múltiples métodos de investigación social, debería ir a su videoclub y alquilar "Los fisgones" (sneakers), con Robert Redford. Es una película emocionante donde un grupo de hackers logra penetrar en una empresa para robar un proyecto secreto. ¿Cómo lo consiguen? Empleando, entre otros métodos, costosos procedimientos de investigación social.

Pero a veces, resulta mucho más sencillo. Precisamente las personas con actividad online suelen revelar mucho sobre ellas mismas, sin darse cuenta. En los grupos de noticias o chats hablan con los demás de lo que les gusta, o lo que les preocupa. ¿Y si el interlocutor es un hacker camuflado que quiere tirarle de la lengua? Muchos internautas poseen su propia homepage, donde divulgan sus hobbies y preferencias. Una inagotable fuente de información para cualquier hacker interesado.



Áreas como esta bajo http://www.deja.com o http://www.google.com permiten la investigación detallada de los usuarios de Internet más activos.

INFO

Robo de contraseñas en los grupos de noticias

En los grupos de noticias se relata un caso absolutamente clásico, donde la investigación social condujo inmediatamente al éxito. Un hombre había elegido el nombre de su perro como contraseña de acceso a su ordenador. Además, era miembro activo de un grupo de noticias sobre el tema "Perro y amo", donde contaba regularmente las gracias de su mascota. Un hacker aprovechó el archivo del grupo de noticias *DejaNews* (http://www.deja.com), para averiguar más datos sobre ese hombre. Encontró contribuciones de su víctima, donde figuraba el nombre del perro. Y probó suerte (con éxito). En el Capítulo 8 nos ocuparemos con más detalle de la investigación personal a través de Internet y también les mostraremos las posibilidades para proteger sus datos personales de esta clase de ataques de espionaje.

Contramedidas: protegerse de la investigación social.

Desgraciadamente, no se puede evitar un ataque por investigación social. La pregunta fundamental que se impone es: ¿cuánto queremos revelar a los demás sobre nosotros a través de Internet? Aquí, la recomendación es simplemente ser un poco reservado con la información realmente personal. Imagine que ante su casa o vivienda, hubiera un tablón de anuncios donde usted pudiera colocar información sobre sí mismo para que la lean los transeúntes. Aquello que jamás expondría al público en ese tablón de anuncios, tampoco lo debería publicar en Internet. ¿Fijaría a ese tablón información sobre valiosos bienes personales, para que a los ladrones no les quepa duda de que vale la pena entrar en su casa?

En la mayoría de los casos, la investigación social apunta hacia los datos de acceso como nombres de usuario y contraseñas. Por eso, emplee contraseñas que no puedan ser descifradas con métodos de investigación social. Estas pueden ser palabras clave que no tengan nada que ver con su entorno personal (son las mejores), o tan personales que un hacker no las pueda averiguar ni con gran esfuerzo. En el Capítulo 2 nos ocupamos más a fondo de cómo elegir contraseñas realmente seguras y el modo de protegerlas con eficacia.

1.3 Chicos malos, "script kids" y saboteadores

En las noticias de la prensa se llama hackers a las personas más variopintas. Desde el prodigio de la informática de 14 años que, con suerte y habilidad, ha conseguido infiltrarse en el ordenador del FBI, hasta los especialistas con abrigos largos y gafas de sol que trabajan para los servicios secretos. En realidad, los hackers pueden ser clasificados en varios grupos que actúan por los motivos más diversos. En este apartado, vamos a intentar definir los diferentes tipos de hackers, así como su modo de proceder y sus intenciones.

Just for fun – chicos con talento que se aburren

Un fenómeno relativamente nuevo aún son los "script kids". Jóvenes (y no tan jóvenes) fanáticos del ordenador que matan el aburrimiento pirateando. Para ellos, el pirateo se ha convertido en un pasatiempo moderno, como podría ser el monopatín o hacer surf en el metro. Andan siempre en busca de nuevos retos y se sienten reafirmados con los éxitos.

INFO

¿Caos el día de Año Nuevo?

Para el día de Año Nuevo del 2001, a algunos adolescentes americanos se les ocurrió algo muy especial. Mediante ataques organizados del tipo "Denial of Service" quisieron paralizar ese día todo Internet. No tenían ningún móvil real y mucho menos una motivación política. Uno de los implicados, confesó que con esa acción sólo quería impresionar a sus amigos. Por suerte, se evitó el sabotaje. Los adolescentes se habían citado en un espacio público de chats, para acordar el modo de proceder concreto. Parece ser que el operador del foro de chat les escuchó y avisó al FBI.

Para convertirse en "script kid", no hace falta mucho. Un ordenador propio con acceso a Internet facilita las cosas, pero en caso de apuro sirven también los PCs de la escuela, la universidad o un cibercafé. Por regla general, los script-kids no son verdaderos expertos. Sólo se apropian de los conocimientos que necesitan en cada momento. Éstos los adquieren de sus camaradas o también, de Internet, trucos e información sobre agujeros de seguridad, que luego simplemente aplican. Antes, esto daba a lo sumo para algún que otro juego de manos. Pero actualmente, ya hay disponible en Internet todo tipo de información, instrucciones y herramientas explosivas. Esta facilidad de acceder a la información necesaria es lo que hace a los "script kids" tan peligrosos.

Los "script kids" se diferencian de los hackers clásicos en su proceder fundamental. Un hacker que prepare un ataque, primero explorará el objetivo y después, elegirá el método de ataque apropiado. Los "script kids" casi siempre lo hacen al revés. Primero viene el método de ataque, quizá porque hayan oído hablar de un nuevo agujero de seguridad o hayan encontrado un nuevo programa en Internet. Sólo después buscarán ordenadores o redes, donde puedan probar y aplicar esos nuevos métodos. Este modo de proceder trae consigo una amenaza ligeramente diferente. En la mayoría de los casos, los "script kids" no atacan a víctimas concretas. Eligen los objetivos de ataque al azar. Esto significa que por ese lado no hay que temer ataques selectivos, pero sí nos podemos convertir a cualquier hora en víctima casual de un ataque. Al final, el peligro es tan grave como en el caso de los hackers clásicos. No se puede vaticinar a nivel general, si los "script kids" van a destruir datos de conseguir infiltrarse. Algunos se limitan a dejar una marca, otros borran o manipulan ficheros alguna vez. Pero como estos intrusos no suelen ser expertos, siempre hay que temer que causen daños por pura casualidad.

Contramedidas: protegerse de los script-kids

No existe ninguna protección enfocada a los "script kids". Tampoco es necesaria. Si uno protege sus sistemas correctamente y con eficacia de cualquier ataque, tampoco a estos agresores les quedarán muchas oportunidades. Es muy importante que se erradiquen las posibilidades de ataque que sean ya de dominio público. Ante todo, se impone cerrar sin demora los agujeros de seguridad en el software empleado y mantenerse al corriente sobre los problemas de seguridad actuales.

Rencor y envidia – compañeros de trabajo envidiosos

En una categoría similar a la de los "script kids" entrarían los hackers ocasionales, que desentierran sus habilidades en circunstancias especiales. Un ejemplo clásico sería el de un compañero de trabajo envidioso que tras sentirse relegado en un ascenso, quiere jugársela al colega que se llevó el puesto. Así que se pone a pensar en cómo podría desacreditar al otro, o hacerle daño de otro modo. Los hackers ocasionales se asemejan a los "script kids" en que muchas veces, no poseen conocimientos sólidos. Sólo han oído hablar de métodos y datos, o saben dónde y cómo conseguir esa información si la necesitan.

INFO

Un hacker en la central nuclear

En enero 2001, hubo que reforzar considerablemente las medidas de seguridad en las centrales nucleares británicas, tras haberse infiltrado un empleado de la propia Seguridad de Planta en el ordenador principal de una central nuclear. Parece ser que a la hora de contratar a este hombre, con varios antecedentes penales en su haber, no se investigó lo suficiente. Con su acto de piratería, este hacker intentó borrar gran número de datos importantes.

Sin embargo, el modo de actuar presenta diferencias importantes. Los hackers ocasionales suelen proceder contra objetivos concretos. Es cierto que también aquí hay prototipos que se acaban de aprender un nuevo truco y lo quieren probar enseguida. Estos suelen ser más bien juegos malabares, con los que se pretende impresionar a compañeros de trabajo y conocidos. Generalmente, no causan daños reales. Pero la mayoría de los ejemplares de esta especie son más peligrosos, ya que su finalidad es hacer daño. Primero sienten la necesidad de perjudicar a un compañero de trabajo, por poner un ejemplo. Después buscan los medios y las posibilidades para hacerlo.

Estos hackers ocasionales pueden ser muy dañinos, especialmente entre sus compañeros de trabajo. A fin de cuentas, son de la casa. No atacan desde fuera, sino desde dentro. Y tienen la gran ventaja de conocer ya mucha información, que un agresor externo tendría que recopilar primero con gran esfuerzo. Están al corriente de los sistemas y el software empleados y conocen las medidas

seguridad básicas. Además, también tienen acceso a muchas áreas que utiliza su víctima, y no sólo hablando en cuanto a organización, sino también de espacio. Una gran ventaja de estos ataques desde dentro es que resulta relativamente sencillo conseguir el acceso físico a los ordenadores atacados.

Contramedidas: protegerse de los hackers ocasionales

En principio, los hackers ocasionales exigen las mismas medidas de seguridad que cualquier otro tipo de atacante. Sin embargo, un potencial de riesgo especial lo causa el peligro de un ataque desde dentro, por ejemplo por un empleado decepcionado o frustrado, que por alguna razón se quiera vengar del empresario o de un compañero de trabajo. Estos individuos de la casa lo suelen tener muy fácil, ya que nadie cuenta con un ataque desde ese flanco y no existen los correspondientes dispositivos de seguridad.

Como regla general, sólo se puede recomendar la inclusión urgente de estos ataques en la planificación y puesta en práctica de medidas de protección. Para cada empleado, esto supone partir de la base de que sus datos no tienen por qué estar seguros en los sistemas de la empresa. Los datos particulares, aunque los permita el empresario, deberían ser protegidos adicionalmente si se les quiere mantener fuera del alcance de compañeros curiosos. Pero también los documentos importantes de la empresa se deberían proteger cuidadosamente si se quiere guardar su confidencialidad y si, en caso de perderse, las consecuencias para el propio puesto de trabajo de uno pudieran ser nefastas.

Hackers clásicos – entusiastas e ideólogos

Los "script kids" y hackers ocasionales de los que nos hemos ocupado anteriormente, son más bien fenómenos marginales en el entorno de los hackers. No porque numéricamente sean tan escasos, sino porque simplemente no pertenecen a la categoría de hackers "verdaderos". Sólo son personas que aprovechan la gran disponibilidad de información y herramientas pensadas para hackers. Empezaron a aparecer con la creciente difusión de Internet y no son hackers verdaderos, aunque ellos se consideren como tales.

Hackers aficionados

Con mucho, el sector más amplio de hackers lo componen los aficionados. Este término no se emplea en sentido peyorativo, sino para dejar claro que estas personas se dedican al pirateo prácticamente como actividad secundaria, es decir, a modo de hobby. Algunos quizá empezaron como "script kids" o hackers ocasionales y que posteriormente descubrieron su pasión por el tema y se dedicaron a él con mayor intensidad. Ejercen el pirateo como un hobby que les divierte. Para algunos, también es una pasión que les promete satisfacción y autoafirmación.

INFO

Lucha contra a la comercialización de Internet

Muchas veces, los hackers luchan por idealismo o creencias políticas. Por ejemplo, varios hackers emplearon bombas de e-mail como herramienta para "vengarse" de personas y empresas a las que creían culpables de la creciente comercialización de Internet. Fueron sus víctimas, entre otros, políticos como el presidente de los Estados Unidos Bill Clinton, o empresas como AOL o MTV. También instituciones públicas, como por ejemplo la CIA, son víctimas muy apreciadas, ya que en este caso se puede contar con gran cobertura de la prensa. Las bombas de e-mail se basan en la idea de llenar la bandeja de entrada de la víctima con muchas noticias o noticias voluminosas, de modo que se desborde y deje de trabajar.

Los aficionados aprenden poco a poco todos los trucos. Para eso emplean sobre todo Internet, donde intercambian información con afines a la causa y se abastecen de nuevas sugerencias y software. Su experiencia y sus conocimientos les convierten en adversarios que hay que tomar en serio. Pero también son muy cautelosos. Pocas veces se embarcan en empresas realmente arriesgadas. Menos aún en acciones que puedan tener como consecuencia una sanción. A fin de cuentas, no tienen ganas de acabar en la cárcel por culpa de su hobby.

Contramedidas: protegerse de los hackers aficionados

Los aficionados se concentran mayormente en agujeros de seguridad que lleven rápidamente al éxito. Estos agujeros pueden haber sido causados tanto por personas como por el software. Si ven que filtrarse en el sistema les exige un esfuerzo mayor, suelen acobardarse. Por eso, para protegerse de estos agresores es importante enseñarles los dientes. Si los aficionados se percatan de que están ante un sistema mantenido y protegido por una persona segura de sí misma, muchas veces se espantan sólo con eso. Los hackers aficionados se limitan a aquellos ataques, que puedan lanzar a través de la Red desde una distancia prudencial. Para perpetrar ataques físicos directos o dedicarse a una costosa investigación social, les faltan medios y tiempo.

Hackers de pura sangre

El hacker pura sangre suele ser un antiguo aficionado, cuyo hobby se ha convertido en el centro de su existencia. Para él, el pirateo es la tarea y filosofía de su vida. Fiel al lema de que "nada está fuera de su alcance", se deja tentar por cualquier reto. Quiere demostrar todo lo que se puede hacer. Algunos hackers pura sangre ven el pirateo como una variante lúdica de anarquismo, otros se esfuerzan seriamente en mostrar los riesgos de seguridad y concienciar a la sociedad sobre los peligros y las oportunidades de las nuevas tecnologías. Muchas veces, también se mezclan ambas motivaciones.

Los hackers pura sangre pocas veces causan verdaderos daños. Dejan su marca o se apropian de datos confidenciales para demostrar el éxito de su ataque. Al ser expertos, el peligro de que originen daños colaterales por casualidad es escaso. Sin embargo, estos hackers están en constante peligro de apartarse del buen camino.

- La vida de un hacker pura sangre en activo no es barata. Necesita hardware, software y los costes online suponen un dineral. Muchas veces, sólo por eso se ha dado el caso de que estas personas hayan acabado en la delincuencia. Y es que resulta muy tentador emplear los conocimientos y las habilidades con fines lucrativos.
- El pirateo puede ser una especie de adicción. Para algunas personas ha adquirido tal importancia, que pueden ser denominadas a todas luces como adictas. Estos hackers pueden perder fácilmente el control durante sus correrías, dejándose arrebatar por el poder que tienen sobre los datos ajenos.

Contramedidas: protegerse de los hackers idealistas

Los hackers pura sangre suelen tocar todos los resortes. Poseen gran capacidad y experiencia. Por eso, saben dónde buscar y encuentran los agujeros de seguridad con suma rapidez. Además, no les asusta realizar acciones de más envergadura si el objetivo merece la pena. Frecuentemente, marcarles el territorio no basta como protección. Esto espolea aún más a algunos idealistas a demostrar que pueden penetrar en cualquier sistema. Sólo un sistema absolutamente hermético está protegido contra ellos. Sin embargo, son escasos los métodos de ataque costosos o que requieran de un gran esfuerzo técnico. En la mayoría de los casos, los idealistas no disponen de los medios necesarios.

TRUCO

Combatir el fuego con fuego

La mejor protección contra los hackers son precisamente los hackers. A fin de cuentas, para saber si una caja fuerte de nuevo diseño es realmente segura, lo mejor es recurrir a un ladrón de cajas fuertes con experiencia. Del mismo modo, si alguien quiere probar la seguridad real de su sistema, lo mejor es someterlo al ataque de un hacker. Por ejemplo, los fabricantes de productos de cifrado y seguridad convocan regularmente concursos, donde ofrecen un premio atractivo a quien sea capaz de jugársela a sus productos. La respuesta a estos tests suele ser muy grande y en muchos casos, las empresas acaban obligadas a desembolsar el premio porque alguien ha encontrado un punto débil. Algunos hackers retirados se ganan la vida hoy como asesores de seguridad y cobran honorarios por perpetrar ataques de prueba contra sus clientes.

Negocios turbios – espionaje y sabotaje

Hay hackers pura sangre que en algún momento de su vida se pasan al campo profesional. Venden sus conocimientos y habilidades a todo aquel que pueda pagarlas. Hay quien simplemente cambia de bando y se convierte en asesor de seguridad. Un ramo que permite ganar mucho dinero. Otros siguen fieles a sus ideales. Sólo que también quieren ganar mucho dinero. Estos hackers son los más peligrosos. Poseen amplios conocimientos y se conocen prácticamente todos los trucos. Además, casi siempre disponen de un equipo técnico muy completo. No se limitan a descifrar contraseñas o infiltrar caballos de Troya. Si no pueden hacerse con el acceso a un ordenador, emplean recursos para intervenir los ordenadores y los vínculos de red e interceptar el tráfico de datos. Como trabajan para empresas competidoras, gobiernos o servicios secretos, también disponen de los medios necesarios para perpetrar ataques que supongan un mayor esfuerzo financiero y técnico.

INFO

Insolente robo de datos en el centro de investigación nuclear

A finales de 1998, hackers chinos penetraron en el famoso centro de investigación nuclear americano Los Álamos. Consiguieron robar cantidades ingentes de valiosos datos de investigación, descargándolos sencillamente desde los servidores FTP. "Se han bajado una pila de documentos de tres pies de altura", según uno de los oficiales a cargo de la investigación. La utilidad de este tipo de acciones es evidente. Países como China, que también trabajan en el desarrollo de armas nucleares, prefieren aprovechar los resultados ya obtenidos por otros países en sus investigaciones, a alcanzarlos por sus propios medios invirtiendo esfuerzo y dinero. Que el ataque no procedía de un hacker particular, queda demostrado por el hecho de que se pudo rastrear la fuente del ataque. Resultó ser un instituto de investigación oficial en Pekín.

Contramedidas: protegerse de los agresores profesionales

Resulta prácticamente imposible protegerse de hackers profesionales que dispongan de un arsenal completo y los medios financieros necesarios. Los sistemas capaces de resistir a estos ataques son tan costosos y complicados que en una empresa económica, por poner un ejemplo, resultarían imposibles de aplicar. A lo sumo, pueden hallarse en el entorno del ejército y los servicios secretos. Pero incluso aquí, jamás existirá una seguridad absoluta.

Lo único tranquilizador de los hackers profesionales es el hecho de que trabajan sólo por dinero. Es decir, únicamente atacan objetivos que les resulten rentables. Por lo que un usuario particular o una empresa pequeña, apenas temen tener que vérselas jamás con esta gente. Pero quien posea datos tan valiosos que supongan un objetivo rentable para el espionaje industrial, debería invertir todo el tiempo y dinero necesarios en medidas de seguridad eficaces que compliquen la vida lo más posible a un agresor.

Information Warfare – guerra en la era de la información

Para finalizar nuestras reflexiones sobre los hackers y sus motivaciones, queremos centrarnos también en un fenómeno de creciente importancia en los últimos tiempos. *Information Warfare*, en español algo así como guerra de la información , describe la guerra por la información o utilizando los recursos de la era de la información. A primera vista, puede sonar como algo muy marcial, sacado de una novela de ciencia-ficción. Pero en realidad, el futuro ya se nos ha echado encima.

INFO

Guerra de información en Oriente Próximo

La importancia que está alcanzando gradualmente la guerra de la información, ha quedado patente por las recientes luchas en Oriente Próximo entre Israel y los palestinos. Durante la fase álgida del conflicto, formaba parte de la vida cotidiana colapsar los servidores web del ejército israelí o los organismos del gobierno mediante ataques "Denial of Service". En el otro bando, los servidores palestinos fueron hostigados desde todo el mundo por bombas e-mail, con lo que también sufrieron averías.

¿Qué consecuencias trae todo esto? En la era de la información, ésta adquiere cada vez mayor importancia. Si en un conflicto una parte evita que la otra difunda su información, logrará una gran ventaja. Por una parte, el adversario no podrá informar a sus propios partidarios. Por la otra, el vencedor en la guerra de la información se hará con el monopolio sobre la misma. Podrá divulgar su punto de vista sobre el conflicto e influir así en la opinión pública mundial, sin que el adversario tenga la menor posibilidad de difundir su propia versión de lo ocurrido.

El conflicto de Oriente Próximo que hemos descrito, demuestra que esta clase de contiendas muchas veces acaban en tablas, es decir, en una completa desinformación. Pero esto sólo es aplicable mientras exista igualdad en las armas y la lucha se desarrolle entre dos partes que tecnológicamente estén en las mismas condiciones. La ventaja de una guerra de información es que (hasta ahora) sólo hay víctimas virtuales y no resultan heridas personas físicas. Pero conforme crezca en importancia la información, esto también podrá cambiar. Cuando los militares empiecen a atacar por ejemplo los nodos de Internet de un país enemigo, la guerra de la información se volverá tan sangrienta como la militar. Aunque en esto ya no tendrán mucho que ver los hackers.

2. Nivel de seguridad 1: ataques locales

2.1 **Entrada a través del botón de conexión** 69
Contraseñas BIOS – ¿protección o agujero de seguridad? 69

2.2 **El administrador de usuarios de Windows** 75
Definir nuevos perfiles de usuario 79
¿Hasta dónde es seguro el administrador de usuarios? 82
Un verdadero control de acceso con eSafe 85

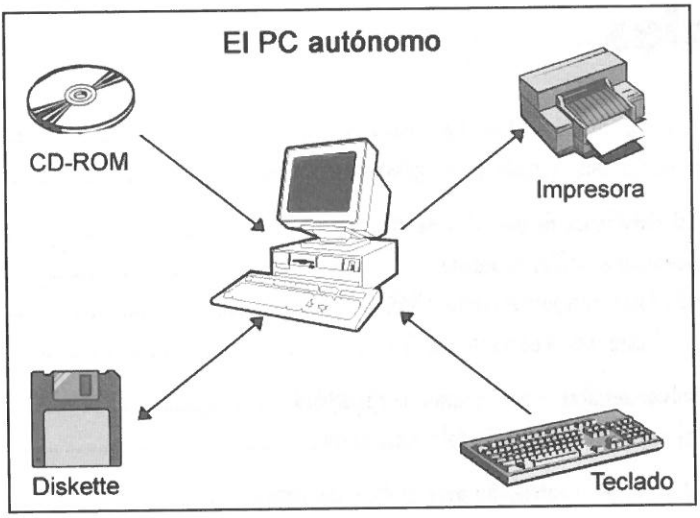
2.3 **El salvapantallas – una trampa de seguridad** 94
Así de segura es la contraseña del salvapantallas 97

2.4 **Protección por contraseña para el PC y los datos** 101
La importancia de las contraseñas 101
Así son seguras las contraseñas 103
Síntomas de que la contraseña ha sido pirateada 109
Contraseñas en aplicaciones y documentos 111

2.5 **Ataques al ordenador por hardware** 114
Señales ópticas y acústicas 115
Radiación electromagnética 116
Interceptar el cable mediante sobreacoplamiento 120

El peligro al que está expuesto un ordenador depende, sobre todo, de los modos de acceso que permita. La solución más fácil de controlar es el PC autónomo, un ordenador sencillo colocado en el hogar o en una oficina, que no dispone de acceso a Internet ni está conectado a ninguna red. El intercambio de datos se desarrolla, fundamentalmente, mediante diversos tipos de dispositivos y soportes removibles. Para introducir datos se pueden emplear disquetes, CD-ROMs, discos ZIP, unidades intercambiables, así como el teclado, un escáner de imagen y otro tipo de unidades de entrada similares. En consecuencia, cualquier peligro para el PC sólo puede partir de estos componentes bien controlados. También los hackers disponen únicamente de este camino para procurarse acceso a un ordenador. Para la salida de datos sirven el monitor, de nuevo los disquetes y otros medios de memoria intercambiable, así como la impresora. Los soportes de sali-

da tienen especial relevancia para los hackers. Sólo a través de ellos pueden sacar del ordenador los datos confidenciales.



El PC autónomo y sus diferentes dispositivos de entrada y salida.

En un PC aislado, los puntos de peligro son perfectamente controlables y, con un poco de esfuerzo, pueden ser vigilados o desconectados. Tenemos, en primer lugar, el peligro de ser infectados con virus o troyanos, peligro al cual está expuesto cualquier PC. Pero en un PC autónomo, un virus sólo puede infiltrarse a través de un soporte de datos removible. Por eso, hay que manejar con mucho cuidado disquetes y CD-ROMs. Nada más insertarlos, sería conveniente someterlos primero a una búsqueda exhaustiva de virus (más información en el Capítulo 3).

Para los hackers y saboteadores, el PC autónomo o aislado supone un reto especial. Para conseguir algo con ellos, no pueden trabajar desde un escondite seguro. Necesitan tener acceso directo al ordenador. Esto siempre encierra un riesgo de seguridad mayor. Además, sus posibilidades de introducir datos para perpetrar los ataques son menores. Para protegerse de ellos, se dispone de varias medidas de software y hardware. Así por ejemplo, se puede proteger el acceso al ordenador mediante BIOS o a través del administrador de usuarios del sistema operativo. Además, como protección adicional de sus datos ante ataques locales, los propietarios de un PC pueden emplear teclados bloqueables, archivadores protegidos para disquetes y otros medios de protección físicos.

En un PC autónomo, los fisgones y espías industriales se encuentran ante las mismas dificultades que los hackers. No disponen de ningún vínculo de red a través del cual puedan espiar un ordenador cómoda y remotamente. En su lugar,

deben adentrarse en el entorno de la víctima para espiar su PC por medios ópticos, acústicos o electrónicos. En este capítulo les mostraremos los puntos débiles de un PC en el ámbito local y cómo pueden ser eliminados aplicando las medidas de protección adecuadas.

2.1 Entrada a través del botón de conexión

El mayor peligro de los PCs locales es la escasa protección. La mayoría de usuarios descuidan las medidas de seguridad más básicas, con lo que abren las puertas de par en par a los agresores. El ejemplo más sencillo y cercano: la mayoría de los PCs pueden ser conectados y arrancados con sólo pulsar el botón de conexión. ¿Y si hace la prueba con su propio PC? ¿Es posible conectar el ordenador, arrancar el sistema operativo y acceder a datos confidenciales o quizá, conectarse a Internet, sin introducir una sola contraseña? Entonces, imagine que su peor enemigo puede acceder durante una hora a ese PC sin que nadie le moleste. ¿Cuánto daño podría causar?

Por todo esto, resulta imprescindible proteger el PC de esta clase de acceso ilimitado; aunque eso suponga tener que teclear una contraseña cada vez que arranque el ordenador. En este apartado, nos vamos a ocupar de la primera línea de defensa contra el acceso no autorizado, la contraseña BIOS. A continuación, pasaremos a la segunda línea de defensa, el arranque de sesión en Windows. Finalmente, detallaremos en el siguiente apartado el administrador de usuarios de Windows, con sus ventajas e inconvenientes.

Contraseñas BIOS – ¿protección o agujero de seguridad?

Independientemente del sistema operativo instalado, todo PC puede ser protegido con una contraseña. La función correspondiente es parte del ***Basic Input Output System*** (BIOS), que es responsable de la primera fase de arranque del ordenador. Ese momento en el que todo tipo de cifras y datos técnicos desfilan por la pantalla a toda velocidad. Hasta que no ha concluido esta fase del arranque, no comienza el arranque del sistema operativo en sí (por ejemplo Windows). Por regla general, esta primera fase de arranque del ordenador puede ser protegida en dos etapas con una contraseña.

- El acceso a los ajustes de la BIOS puede ser protegido con una petición de contraseña. De modo que sólo las personas autorizadas, que conozcan esa contraseña, puedan modificar los ajustes de la BIOS.
- La BIOS puede solicitar una palabra clave en cuanto comience el proceso de arranque y seguir adelante sola, si ha sido introducida la contraseña correcta.

Sobre todo, este último punto es de vital importancia, ya que con una función de este tipo se puede limitar eficazmente el acceso al ordenador. La petición de contraseña tiene lugar antes de que se pueda acceder a los discos duros incorporados. Es decir, quien no introduzca la contraseña correcta no tendrá ninguna oportunidad de acceder a los datos almacenados.

Protección del PC mediante una contraseña BIOS

Si usted quiere configurar una contraseña BIOS, deberá adentrarse en lo más profundo de la configuración BIOS de su ordenador. Por lo que le recomendamos encarecidamente que consulte antes el manual de instrucciones. Intervenir en la BIOS no está del todo exento de riesgo. El simple desajuste de una opción aparentemente insignificante podría desestabilizar su ordenador, o hacer incluso que no arranque. Infórmese bien sobre las opciones que controlan la seguridad de la contraseña. Desgraciadamente, hay programas BIOS de varios fabricantes y en diferentes versiones, por lo que no podemos describir cada detalle. Le enseñaremos cómo ajustar la contraseña BIOS utilizando la ampliamente extendida Award-BIOS. Básicamente, las funciones BIOS de otros fabricantes trabajan de modo similar, aunque pueden tener una estructura diferente o emplear otras definiciones. Si su ordenador va equipado con el BIOS de otro fabricante, ¡consulte sin falta el manual de instrucciones!

INFO

Configuración inglesa del teclado

El programa de setup BIOS se ejecuta nada más arrancar el ordenador, antes de que pueda ser cargado el controlador español del teclado. Esto implica que por ejemplo determinadas teclas, como la *ñ* estarán cambiadas y muchos signos de puntuación no estarán en el lugar habitual. Esto no tiene mayor importancia, ya que usted necesitará, principalmente, las teclas del cursor y muy pocos números y letras. Sólo hay que tener cuidado con las peticiones de confirmación. Deben ser contestadas siempre con *Y* para *Yes* (Sí) o *N* para *No* (No).

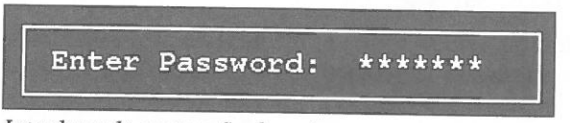
1. Durante la fase de arranque de su PC, aparecerá algún tiempo en pantalla el mensaje *Press DEL to enter SETUP*. Mientras se encuentre en ese punto, podrá activar la BIOS con la tecla *[Supr]*.

Mientras aparezca este mensaje, usted podrá abrir los ajustes de la BIOS.

2. Utilizando las teclas del cursor, seleccione en el menú principal el apartado *SUPERVISOR PASSWORD* y actívelo con *[Intro]*.

Bajo SUPERVISOR PASSWORD, podrá colocar la contraseña para acceder a la BIOS.

3. A continuación, aparecerá un campo de entrada de datos, donde podrá introducir la contraseña con la que pretenda proteger el acceso a los ajustes de la BIOS. Introduzca ahora la contraseña y confírmela con *[Intro]*. Es importante que emplee una contraseña lo más segura posible (lea al respecto también uno de los siguientes apartados de este capítulo).



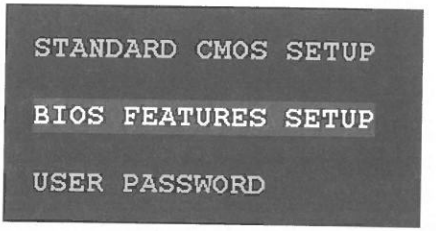
Introduzca la contraseña deseada.

4. Acto seguido, aparecerá un segundo campo de entrada de datos donde deberá introducir otra vez la contraseña, para excluir un posible error de mecanografía y confirmarla.

Para más seguridad, vuelva a introducir la contraseña.

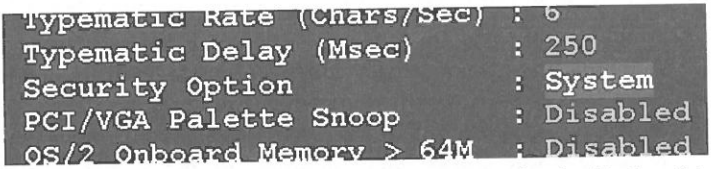
5. Repita este proceso con la opción *USER PASSWORD*, para fijar la contraseña que limitará el acceso a su ordenador. Puede introducir la misma contraseña u otra diferente.

6. Luego, seleccione en el menú principal la opción *BIOS FEATURE SETUP*.



Seleccione BIOS FEATURE SETUP para establecer el nivel de seguridad de su PC.

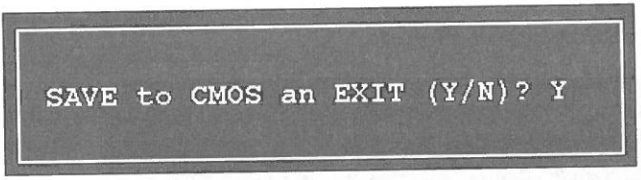
7. Busque aquí, entre las distintas configuraciones de BIOS, la opción *Security Option*. Con al opción *Setup* activará la protección por contraseña, pero sólo para el acceso a BIOS. Si por el contrario selecciona *System*, cada vez que arranque su ordenador, éste le pedirá la *User Password* (contraseña de usuario).



Así logrará que cada vez que arranque el ordenador, éste le pida la palabra clave.

8. Salga del menú con *[Esc]*.

9. A continuación, seleccione en el menú principal la opción *SAVE & EXIT SETUP*, contestando la petición de confirmación posterior con *Y* para *Yes* (¡teclado inglés!). Esto grabará los cambios realizados y rearrancará el ordenador. En este nuevo arranque, se le pedirá por primera vez que introduzca la contraseña.



Para concluir, confirme si quiere guardar los cambios.

Con esto, el acceso a su ordenador queda protegido por contraseña. Tenga en cuenta que a partir de ahora, sólo podrá acceder a él con esa contraseña. Si la olvida, tampoco podrá entrar ya en la configuración de la BIOS para desactivar la función e introducir una nueva palabra clave. Con lo que le resultará difícil acceder a su ordenador, aunque no del todo imposible, como demuestra el siguiente apartado.

¿Hasta qué punto es fiable la contraseña BIOS?

A pesar de todo, las contraseñas BIOS tienen una seguridad limitada; una buena noticia, si ha olvidado su contraseña y se ha cerrado a sí mismo el acceso al ordenador. Pero para todos los demás significa que la contraseña BIOS sólo protege sus datos limitadamente. Esta función de seguridad puede ser anulada de varias formas:

Burlar la contraseña por hardware

La mayor parte de los programas BIOS poseen, por razones de seguridad, una función de recuperación. Esta función se activa automáticamente, por ejemplo, si está vacía la batería cuya corriente sirve para grabar las configuraciones de la BIOS. Esto apenas ocurre durante la vida útil normal de un PC, pero puede ser provocado artificialmente en cualquier momento. Desconectando la batería durante algunas horas, la memoria perderá los datos almacenados, tras lo cual toda la BIOS volverá a la configuración inicial de fábrica, es decir, sin protección por contraseña. Después de esto, se podrá acceder sin restricciones.

Por otro lado, muchas placas base ofrecen una función de reset, que no se corresponde precisamente con la tecla Reset de la carcasa. Con esta característica, ni siquiera es necesario retirar la batería, tan sólo hace falta desviar determinado contacto mediante un *jumper* durante un breve periodo de tiempo, y así restaurar los ajustes de fábrica. Esta función es una medida de protección que resucita el PC en cualquier circunstancia, incluso si la configuración de la BIOS ha sido machacada por un uso incorrecto o un defecto técnico. Pero, por desgracia, también es la puerta trasera por la que los hackers pueden hacerse con el acceso al ordenador.

Para protegerse de estos ataques al hardware, sólo existen medidas adicionales que bloquean físicamente la carcasa del ordenador y el teclado. La carcasa del PC puede ser protegida con candados, de modo que para acceder a la batería y los circuitos de restauración sólo quede ya la fuerza bruta. Para el teclado, se dispone de medidas de protección similares, aunque éste sea bastante más difícil de proteger por tratarse de un dispositivo adicional que va conectado. Al final de este capítulo, entraremos más a fondo en los ataques a PCs a través del hardware.

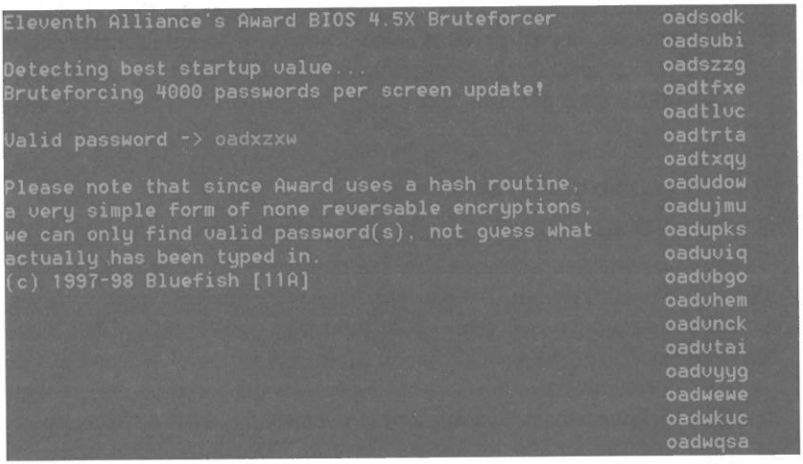
Burlar la contraseña por software

Si se posee la experiencia necesaria, ni siquiera hace falta recurrir al destornillador para reventar la contraseña BIOS. Como muchos otros creadores de software, los fabricantes de BIOS dejan muchas veces puertas traseras en sus funciones de password, ya que éstas están pensadas para ayudar a los usuarios que hayan olvidado su contraseña y ya no puedan arrancar el ordenador. Estas puertas traseras son contraseñas maestras especiales que siempre serán aceptadas por la BIOS, sin importar la que eligiera el usuario. Lo ideal de estas puertas traseras sería que fueran absolutamente secretas. Pero la realidad es muy distinta. Usted puede comprobar fácilmente si existe una contraseña maestra para su propio PC y versión de BIOS correspondiente. En Internet existen numerosas páginas web que permiten consultar listas de contraseñas maestras conocidas, por ejemplo en http://www.cracking.de/files/bioscodes.txt.

Programas para descifrar BIOS

Para concluir, existen programas especiales que leen de la BIOS las contraseñas guardadas. Realmente, no sirven de mucho si se tiene el ordenador desconectado o no hay manera de acceder a él. Pero, una vez en funcionamiento, un intruso podría ejecutar uno de estos programas y averiguar la contraseña guardada en la BIOS. ¿Por qué no comprueba si su PC también se deja engañar por uno de estos programas? Además, puede resultar muy práctico para cuando realmente haya olvidado la contraseña de acceso a la BIOS. Un programa de este tipo es el *!BIOS*, de carácter gratuito, que se puede descargar desde la dirección http://www.11a.nu/ibios.htm. Este programa ofrece la ventaja de reunir una amplia gama de herramientas enfocadas a este objetivo. Con este software es posible desencriptar casi todas las contraseñas BIOS. Huelga decir que un programa así sólo debe ser ejecutado en el propio PC, o con el permiso del correspondiente propietario.

El manejo de !BIOS es sumamente sencillo. Usted sólo debe indicar el fabricante de su BIOS. El programa le presentará los módulos disponibles para esa versión BIOS. Elija uno de ellos y hágale trabajar. Lo mejor es que pruebe simultáneamente varios módulos o incluso todos los disponibles, anote los resultados y después, haga la prueba. No todos los métodos arrojan los resultados correctos para todas las versiones de BIOS, pero la experiencia ha demostrado que siempre hay una contraseña apropiada.



Con los módulos Crack de !BIOS, se pueden extraer por lectura la mayoría de contraseñas BIOS.

Un pequeño apunte adicional acerca de las contraseñas averiguadas. Casi siempre son combinaciones numéricas caóticas que en la mayoría de los casos, no tienen nada que ver con la contraseña que se introdujo. Aún así, permiten el acce-

so a BIOS o al ordenador por una sencilla razón: las contraseñas están almacenadas en BIOS como suma de comprobación, es decir, a partir de la contraseña introducida se genera un número. Esta derivación de la suma de comprobación a partir de la contraseña es unívoca. Esto significa que a partir de una contraseña, sólo se puede derivar una suma de comprobación. A la inversa, sin embargo, la cosa cambia: a partir de una suma de comprobación se pueden derivar varias contraseñas. Dicho en otros términos: contraseñas totalmente diferentes pueden conducir a la misma suma de comprobación. Los fisgones de contraseñas siempre acaban encontrando alguna combinación de letras que les conduzca a la suma de comprobación guardada en la BIOS. Al introducir esa combinación, la BIOS averiguará la suma de comprobación, la comparará con la cifra guardada y constatará la coincidencia. Desde el punto de vista de la BIOS, con esto ha sido introducida la contraseña correcta.

2.2 El administrador de usuarios de Windows

A partir de la versión 95, el sistema operativo de Windows dispone de un administrador de usuarios integrado. Su función primordial es permitir que diferentes usuarios tengan una configuración individual sobre un mismo PC. Aparte de esto, protege los datos confidenciales como e-mails y favoritos web. En combinación con unas directrices para el sistema, aún puede hacer más. Por ejemplo, permite limitar individualmente el acceso de determinados usuarios a ciertas configuraciones del sistema. Para que esto sea posible, los usuarios deben registrarse al comienzo de cada sesión con su nombre y contraseña.

Windows reconoce a los usuarios por este logon o login y les asigna las configuraciones y opciones de escritorio que ellos guardaran al finalizar su última sesión de trabajo. Del mismo modo, durante el inicio de sesión activa las limitaciones de acceso que fueran definidas por el administrador del ordenador.

INFO

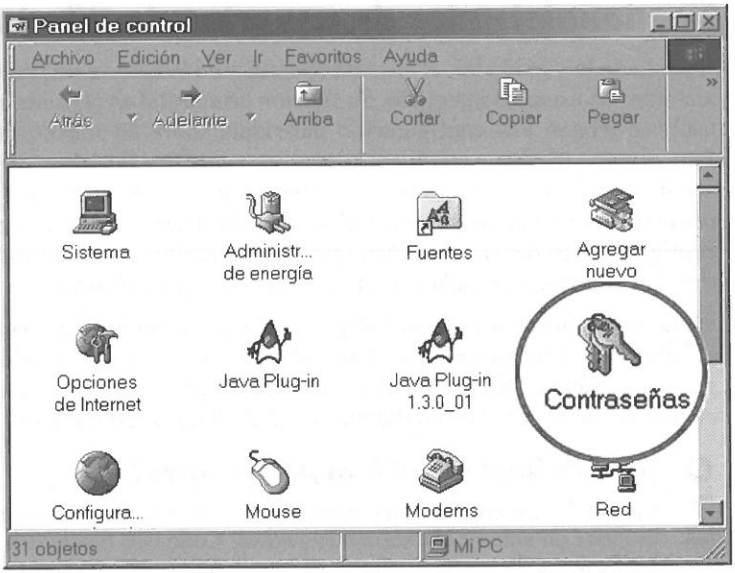
¿Cuál es la función principal de los perfiles de usuario?

Los perfiles de usuario van encaminados, ante todo, a proporcionar a los usuarios un entorno de trabajo individual. Cada uno puede definir sus propios colores de pantalla, ajustar su propio fondo, elegir un protector de pantalla individual, etc. Estos datos son almacenados en su perfil y activados cada vez que inicie una sesión. Sin los perfiles de usuario, cada cambio que se hiciera en el entorno de trabajo o escritorio, afectaría a todos los usuarios. Después del arranque, cada uno tendría que reajustar el sistema según sus necesidades. Aparte de esto, los perfiles de usuario ofrecen cierta confidencialidad en aplicaciones de comunicación como Internet Explorer o Outlook Express. También aquí se almacenan los datos personales en el perfil de usuario. De modo que, varios usuarios podrán compartir un navegador web y un programa de correo electrónico, pero gracias a los perfiles, a cada usuario sólo le aparecerán sus noticias y sus favoritos web. Los datos del resto de usuarios le serán invisibles.

Activar el administrador de usuarios de Windows

Los sistemas Windows pueden trabajar enteramente sin administrador de usuarios. Por ejemplo, no hace ninguna falta si en un ordenador sólo trabaja una persona. Usted puede comprobar fácilmente si su PC tiene activado el administrador de usuario por el comportamiento de arranque de Windows. Si al entrar en Windows no se le exige identificador de usuario ni contraseña, el administrador de usuario no estará activado. Si por el contrario el sistema se los pide, significará que el administrador de usuarios sí está activado. De no estarlo, podrá lograrlo procediendo del siguiente modo:

1. Abra, con *Inicio/Configuración/Panel de control*, el panel de control de Windows y haga doble clic sobre el icono *Contraseñas*, que abrirá las configuraciones para el administrador de usuarios.



Tras el icono Contraseñas, se oculta la activación del administrador de sistemas.

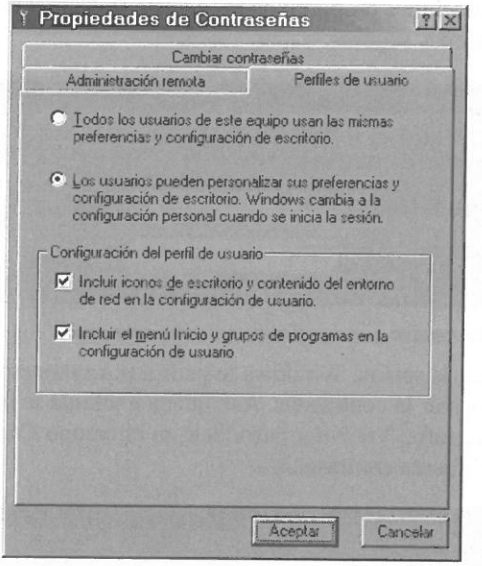
2. En la ventana de *Propiedades de Contraseñas*, escoja la pestaña *Perfiles de usuario.*

3. Aquí, active la opción *Los usuarios pueden personalizar sus preferencias y configuración de escritorio. Windows cambia a la configuración personal cuando se inicia la sesión.*

4. Además, marque la opción *Incluir iconos de escritorio y contenido del entorno de red en la configuración del usuario*, dentro del apartado

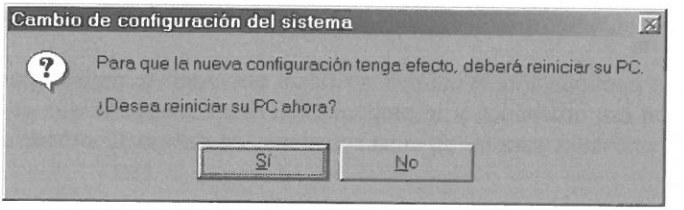
Configuración del perfil de usuario. De este modo, introducirá para cada usuario sus configuraciones individuales con respecto al escritorio de Windows.

5. Active, finalmente, la opción *Incluir el menú Inicio y grupos de programas en la configuración de usuario*. Así creará para cada usuario un menú de inicio individual con sus propios grupos de programas.



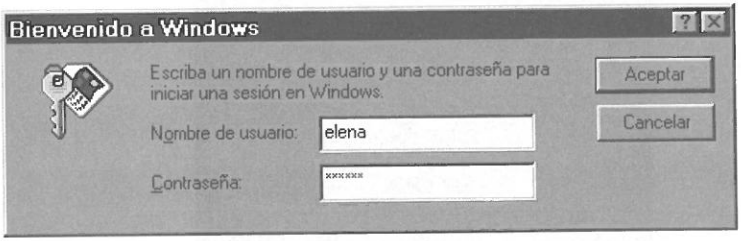
Con estas opciones podrá activar el administrador de usuarios de Windows.

6. Confirme las nuevas configuraciones con *Aceptar*. Para que el administrador de usuarios quede definitivamente activado, es necesario reiniciar el ordenador. Windows emitirá el mensaje correspondiente. Confirme el rearranque con el botón *Sí* tras haber cerrado todos los archivos que pudieran quedar abiertos.



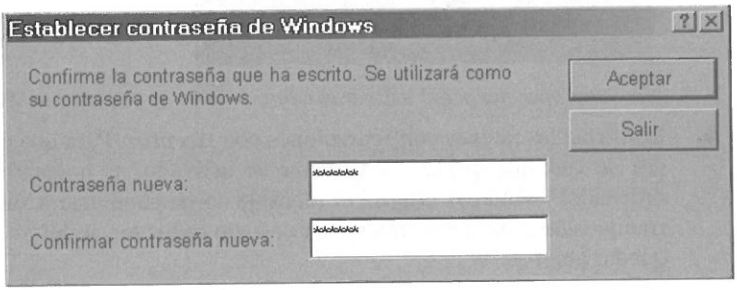
Una vez introducidas las modificaciones, habrá que reiniciar Windows.

7. Espere a que Windows inicie de nuevo.
8. Como tras el rearranque ya estará activado el administrador de usuarios, deberá registrarse como tal. Windows le propondrá un nombre de usuario derivado de los datos personales que indicó al instalar Windows. Acepte esa sugerencia o elija el nombre que le parezca más apropiado.
9. Indique, además, una palabra clave. A la hora de escogerla, por favor tenga en cuenta las instrucciones proporcionadas en este mismo capítulo sobre la elección de contraseñas seguras.



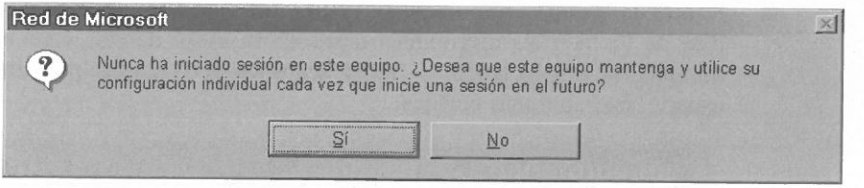
Desde este momento, tendrá que registrarse en cada arranque.

10. En el primer inicio de sesión, Windows le pedirá por razones de seguridad que vuelva a confirmar la contraseña. Así, queda excluida la posibilidad de errores de mecanografía. Vuelva a introducir en el campo *Confirmar contraseña nueva* la misma contraseña.



Para mayor seguridad, repita la contraseña cuando la introduzca por primera vez.

11. A continuación, Windows verificará que usted se registra por primera vez en ese ordenador y le preguntará si desea conservar sus configuraciones personales para las siguientes sesiones de trabajo. Confírmelo con *Sí*.



La primera vez que se registre un usuario, Windows creará un nuevo perfil de usuario individual.

Acto seguido, Windows creará un perfil propio para el nuevo usuario, donde guardará todas las configuraciones personales. Con esto, usted habrá activado el administrador de usuarios de Windows y se habrá registrado como usuario. Para usted no va a cambiar nada, salvo que desde ahora tendrá que registrarse cada vez que arranque el sistema. Sin embargo, a partir de este momento podrá definir perfiles individuales para otros usuarios.

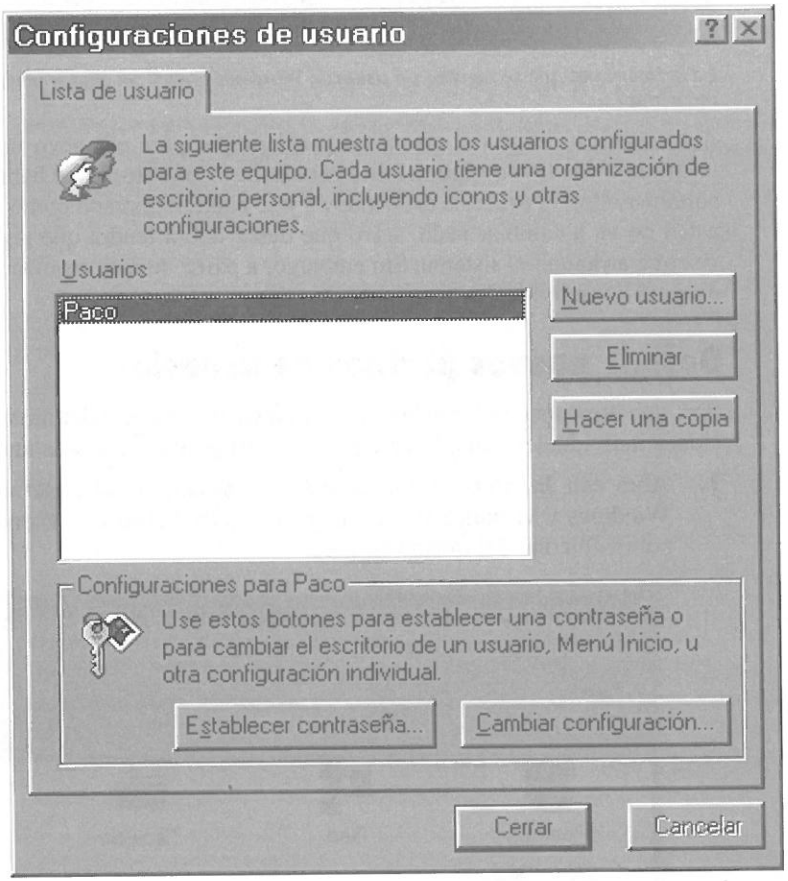
Definir nuevos perfiles de usuario

Para que otros usuarios puedan trabajar en su ordenador y definir sus configuraciones individuales, tendrá que crear un perfil propio para cada uno.

1. Abra con *Inicio/Configuración/Panel de control* el panel de control de Windows y visualice las configuraciones de *Usuario*, haciendo doble clic sobre el icono del mismo nombre.

Tras el icono Usuarios se ocultan las configuraciones para los perfiles de usuario.

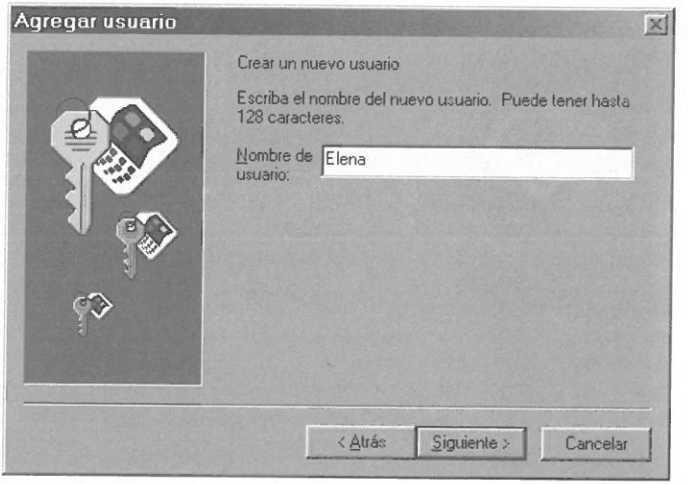
2. Dentro del menú Configuraciones de usuario, verá en el campo Usuario una lista de los perfiles disponibles hasta ahora. Aquí debería figurar, como mínimo, su propio perfil. Si usted acaba de activar el administrador de usuario, no habrá más perfiles.



Aquí se administran los perfiles de usuario.

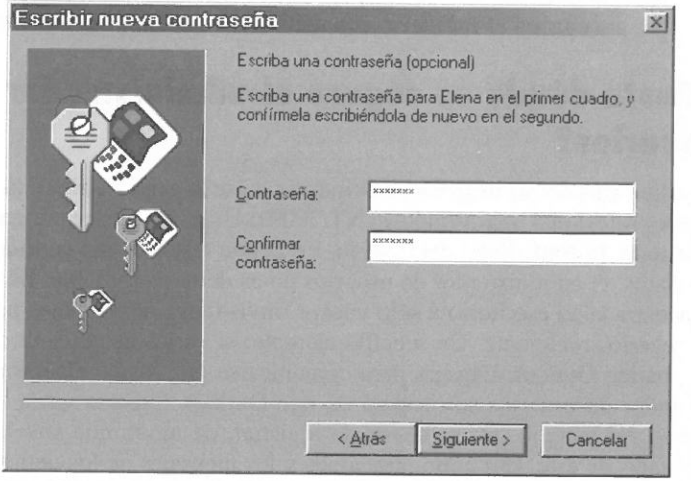
3. Para generar un nuevo perfil de usuario, haga clic sobre el botón *Nuevo usuario*. Ahora le aparecerá un asistente que le guiará durante la definición de nuevos perfiles. Abra la ventana de introducción del asistente, haciendo clic sobre el botón *Siguiente*.

4. En primer lugar, cree para el nuevo usuario un nombre, con el que éste se tendrá que registrar cada vez que arranque el sistema en el futuro.



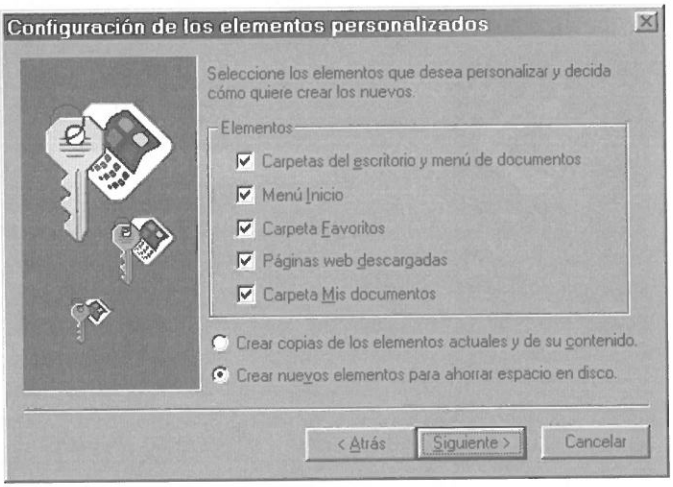
Introduzca un nombre para el nuevo usuario.

5. A continuación, introduzca la *contraseña* con la que el usuario nuevo se identificará cuando se registre. Introdúzcala de nuevo en el campo *Confirmar contraseña*.



Introduzca la contraseña del nuevo usuario.

6. Ahora, defina qué partes del escritorio deben ser adaptadas individualmente para ese usuario. Para ello, deberá marcar todas las opciones en el apartado *Elementos* y seleccionar la opción *Crear nuevos elementos para ahorrar espacio en disco*.



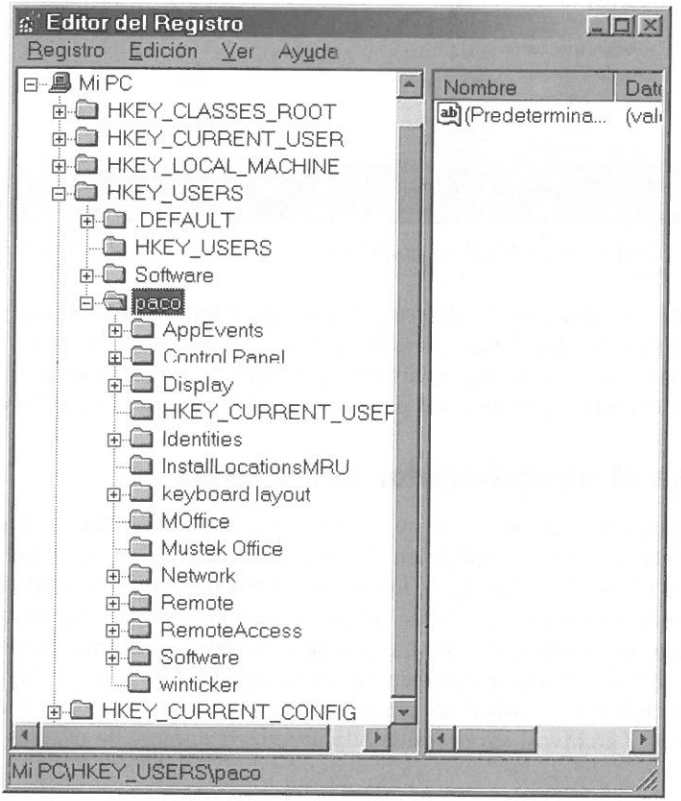
Determine qué elementos deben ser definidos individualmente para ese usuario.

7. El último paso será hacer clic sobre *Finalizar*, para cerrar el asistente. Windows generará ahora el perfil del nuevo usuario que, a partir de ahora y cada vez que arranque el sistema, podrá registrarse con su nombre de usuario definido y su correspondiente palabra clave. De esta forma, siempre encontrará el escritorio adaptado a sus necesidades individuales.

¿Hasta dónde es seguro el administrador de usuarios?

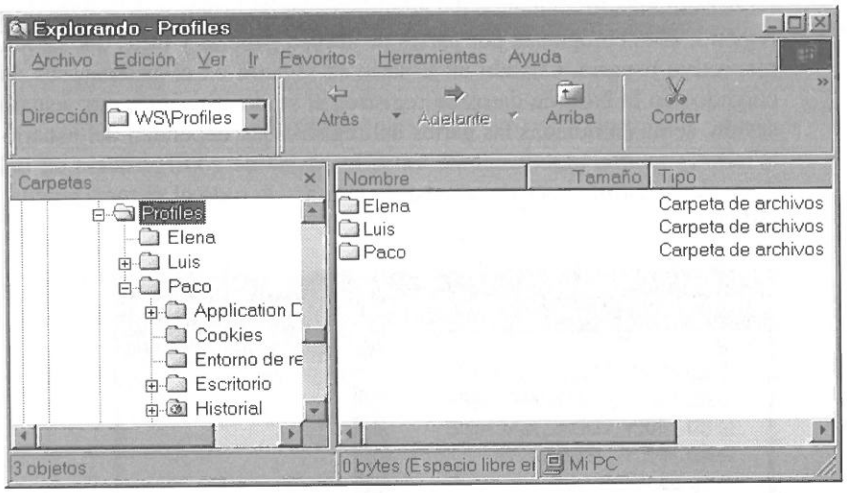
Al administrador de usuarios de Windows no se le exige la seguridad de un ordenador profesional bajo Windows NT/2000 o Unix. Lo que se pretende es buscar, ante todo, la comodidad del usuario. En lo que respecta a la confidencialidad de los datos, el administrador de usuarios no es demasiado fiable. Básicamente, se concentra en el escritorio y sólo vuelve "invisibles" ciertos datos personales, sin protegerlos realmente. Un sencillo ejemplo: si varios usuarios de un ordenador comparten Outlook Express para comunicarse por correo electrónico, el administrador de usuarios se ocupará de que Outlook Express vacíe la bandeja de correo del usuario que se acabe de registrar, de modo que sólo aparezcan los mensajes de éste. Las configuraciones y los mensajes de los demás usuarios no podrán verse. Sin embargo, están ahí y el usuario que esté registrado en ese momento, podrá leer los mensajes de los otros utilizando Explorer. Esto requiere algunos conocimientos sobre el sistema pero sabiendo dónde buscar, se puede hacer sin mayor problema.

La herramienta fundamental del administrador de usuarios es la base de datos de registro. Está compuesta por partes de acceso general y otras que dependen del respectivo usuario. Cuando un usuario se registra en el sistema, sus datos son cargados en la base de datos de registro. Si se desconecta y otro usuario inicia sesión, serán cambiadas las partes del registro que dependan del usuario. Como Windows guarda prácticamente todos los datos de configuración en la base de datos de registro, se puede adaptar de este modo todo el sistema a cada usuario individual.



La prueba: en el editor de registro sólo aparecen los datos del usuario registrado en ese momento...

Pero esto no quiere decir, que no sean accesibles los datos de los demás usuarios. Basta con abrir la carpeta *C:\Windows\Profiles*, para acceder a los datos de todos los demás usuarios registrados en el PC. No es que aquí los formatos de datos sean precisamente fáciles de leer, pero si se sabe lo que se busca, puede encontrarse sin mayor problema.



... pero en el Explorador de Windows también se puede acceder a los datos de todos los demás usuarios.

En resumen, el administrador de usuarios sólo sirve limitadamente para guardar los datos con seguridad. Evita que alguien tropiece por casualidad con los datos confidenciales que usted tenga guardados y complica un poco más la vida a los fisgones. Pero no proporciona una protección real de sus archivos personales.

Saltarse el administrador de usuarios

El administrador de usuarios se puede "burlar" con relativa facilidad. Seguramente, ya habrá reparado en el botón *Cancelar* que se encuentra en la ventana de inicio de sesión. Si es lo bastante curioso como para probarlo, verá que haciendo clic sobre ese botón se puede cancelar el proceso de registro. Aunque esto no quiere decir que quede interrumpido todo el proceso de arranque. Al contrario, Windows arranca de todos modos, sólo que sin registro de usuario y con las configuraciones estándar. Tras lo cual tendrá acceso a todas las aplicaciones y archivos, sin necesidad de introducir nombre de usuario ni contraseña.

Del mismo modo, durante el inicio de sesión podrá introducir, sin más, cualquier nombre de usuario y contraseña. Windows le dará la bienvenida como usuario nuevo, le definirá su propio perfil de usuario y a continuación, le concederá acceso a todos los recursos. ¿Para qué forzar la contraseña, si es tan fácil entrar?

De todo esto se desprende que el administrador de usuarios va enfocado principalmente a la administración y no tanto a la seguridad. Aunque también hay que decir que este es uno de los argumentos principales que emplea Microsoft para

diferenciar su serie Windows 9x/ME de los productos más profesionales como Windows NT/2000. No obstante, existe la posibilidad de establecer en Windows 9x o ME un nivel de seguridad absolutamente comparable al de las versiones profesionales de Windows. Para lo cual, será necesario complementar al administrador de usuarios de Windows con un software adecuado, que no se limite a ocultar archivos sino que también los bloquee para usuarios no autorizados. A continuación, vamos a presentar una solución de este tipo. Si desea saber más acerca de alternativas como Windows NT o 2000, le recomendamos echar un vistazo al Capítulo 10.

Un verdadero control de acceso con eSafe

El producto eSafe aparece en diferentes partes de este libro en relación con diversas tareas. Esto ya indica que se trata de un sistema muy completo y que cubre prácticamente todos los aspectos de seguridad de un PC. En el Capítulo 3, detallamos cómo probar con eSafe y sin riesgos, programas nuevos o desconocidos. En el Capítulo 4, presentamos a eSafe como una solución firewall o cortafuegos, flexible para cualquier PC con conexión a Internet y en el mismo punto, se describe detalladamente la instalación y el manejo del software. Pero eSafe no sólo es capaz de proteger del acceso ilícito a los datos contenidos en su PC, sino también de usuarios no autorizados. En las páginas siguientes vamos a mostrarle cómo emplear eSafe, junto con el administrador de usuarios de Windows, para proteger eficazmente las unidades de disco, los directorios o los archivos importantes del acceso no autorizado por parte de otros usuarios.

INFO

Así vigila eSafe a los usuarios

Con el administrador de usuarios de eSafe, se puede definir con exactitud para cada usuario de un ordenador, qué derechos de acceso posee y sobre qué discos o directorios. eSafe vigilará a los usuarios registrados. Antes de conceder cualquier acceso a un archivo, comprobará las reglas establecidas para ese usuario. Si éste intenta entrar en un archivo para el que no está autorizado, eSafe bloqueará ese acceso. Al programa con el que se haya intentado acceder, le parecerá que el archivo solicitado no puede ser abierto debido a un error de archivo. Así que reaccionará con un mensaje de error. El usuario ni siquiera advertirá que el archivo deseado le está siendo ocultado por un mecanismo de protección especial. eSafe cambiará ahora al administrador de usuarios de Windows. Desde allí, averiguará quién es el usuario que está dado de alta en ese momento y activará el correspondiente conjunto de reglas. Es decir, para que eSafe pueda realizar correctamente su función protectora, primero deberá haber sido activado el administrador de usuarios Windows. Además, todos los usuarios que deban ser vigilados por eSafe, tendrán que haber sido definidos bajo Windows (según lo descrito anteriormente).

Controlar a los usuarios de Windows con eSafe

Para definir a los usuarios y regular sus derechos de accesso, acceda a las configuraciones de eSafe haciendo clic sobre el botón *Opciones* de la ventana de control. En el siguiente menú elija *Configuración avanzada*. Si desea introducir un nuevo usuario, deberá seguir dos pasos:

- La creación de un conjunto de reglas que decida los discos, directorios y archivos a los que podrá tener acceso el usuario. También se puede emplear este tipo de conjunto de reglas para varios usuarios. Es decir, usted podrá crear un conjunto general válido para todos los usuarios.
- La definición del usuario y la asignación de uno o varios conjuntos de reglas, que limiten sus actividades en el ordenador.

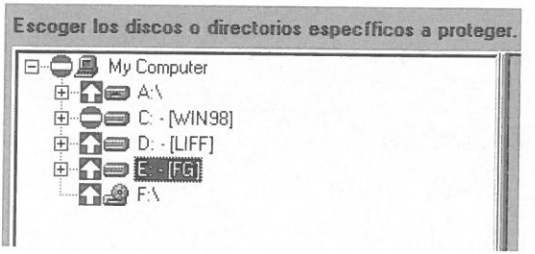
Generar un conjunto de reglas para usuarios

En primer lugar, hay que definir los discos, directorios y archivos sobre los que no se permitirá acceso al usuario. Durante la instalación, eSafe ya creó algunos de estos conjuntos de reglas para las aplicaciones conocidas que encontró en su ordenador. Pero usted también puede crear, en todo momento, conjuntos de reglas propias. En nuestro ejemplo, queremos denegar a los usuarios todo acceso a la unidad *G*, porque ahí es donde guardamos nuestros datos personales que no importan a nadie más.

1. Abra en las configuraciones de eSafe el apartado *Protección de recursos*.
2. En la lista de selección, bajo *Conjuntos de Protección de Recursos*, elija el conjunto de reglas *Blank* (vacío) para que le sirva de base. En principio, este conjunto permite un acceso totalmente ilimitado. Sólo se prevén restricciones en el índice de programas del propio eSafe, para evitar que éste pueda ser anulado borrando archivos de programa importantes.

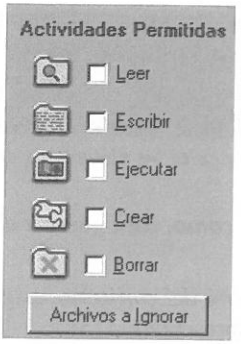
Lo mejor es que elija el conjunto de reglas vacío Blank, que le servirá de base para crear sus propios conjuntos de reglas.

3. Para proteger a la unidad *G*: de nuestro ejemplo, márquela en la lista bajo *Escoger los discos o directorios específicos a proteger.*



Seleccione los discos, directorios y archivos para los que pretenda bloquear el acceso.

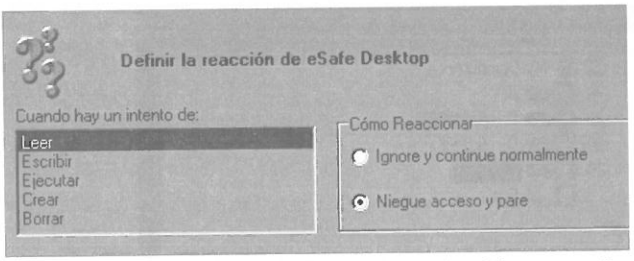
4. Establezca en la zona derecha de la sección *Actividades Permitidas*, qué accesos se le permitirán al usuario sobre los recursos seleccionados en la parte izquierda. Para seguir con nuestro ejemplo, si quiere bloquear totalmente el acceso a una unidad, simplemente desactive todas las opciones.



Así se establecen las restricciones de acceso.

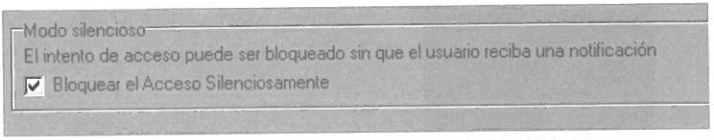
5. Ahora, cambie a la categoría *Cómo reaccionar*, para definir cómo debe proceder eSafe en caso de violación de las restricciones de acceso establecidas.

6. Para todos los tipos de acceso enumerados a la izquierda, bajo *Cuando hay un intento de*, seleccione a la derecha, en el apartado *Cómo Reaccionar*, la opción *Niegue acceso y pare*, para que eSafe evite eficazmente las violaciones de las reglas.



Decida cómo debe comportarse eSafe en caso de violar una regla.

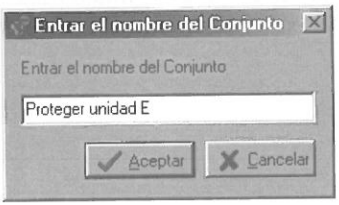
7. Si, además, activa la casilla del apartado inferior *Bloquear el Acceso Silenciosamente*, no se advertirá al usuario sobre las violaciones de las reglas. Éstas serán bloqueadas sin explicaciones. Así, los usuarios no se percatarán de que están siendo controlados. Las infracciones sólo quedarán reflejadas en el protocolo, donde usted las podrá analizar posteriormente.



En el Modo silencioso, eSafe trabaja oculto y evita las violaciones de reglas sin hacer comentarios.

8. Ahora, haga clic sobre el botón *Salvar como*, para guardar el conjunto de reglas generado.

9. En el cuadro de diálogo *Entrar el nombre del conjunto*, asigne al conjunto de reglas un nombre apropiado y representativo. Si usted ha creado el conjunto expresamente para un determinado usuario, podrá emplear el nombre de este usuario. También existiría la posibilidad de denominar al conjunto en función de sus repercusiones (por ejemplo: sin acceso a la unidad G:). Esto resulta especialmente útil si quiere asignar, desde el principio, un conjunto de reglas a varios usuarios. Elija un nombre y guarde el conjunto de reglas con *Aceptar*.



Introduzca un nombre apropiado para el nuevo conjunto de reglas.

TRUCO

Definir un conjunto de reglas eficaz

A la hora de definir conjuntos de reglas, se debe sopesar qué derechos necesita el usuario para poder trabajar con eficacia y qué restricciones hacen falta, para evitar que los propios datos sean puestos en peligro. Para ello, habría que diferenciar tres áreas:

- Por regla general, los usuarios necesitan espacio para guardar sus propios datos. Si no lo tienen, no pueden trabajar con eficacia. Por lo que cada usuario debería tener permiso de escritura para un directorio o unidad como mínimo. Por eso, lo mejor es crear un directorio especial para cada usuario, sobre el cual pueda tener todos los derechos.
- Para poder trabajar en un ordenador, los usuarios deben tener derecho a utilizar determinadas secciones del sistema operativo y las aplicaciones instaladas (p.ej. un procesador de textos). Con este fin, habrá que concederles al menos autorización para leer los directorios correspondientes. Aquí se incluyen por ejemplo carpetas como *C:\Windows* o *C:\Archivos de Programa\Microsoft Office*.
- Finalmente, hay áreas a las que jamás deberá permitirse el acceso a otros usuarios, por contener datos confidenciales o aplicaciones que no deban arrancar otros usuarios. Aquí, es imprescindible que para estos discos y directorios se retiren los derechos de acceso a los usuarios no autorizados.

Para las áreas que no se dejen clasificar claramente en estas tres categorías, rige lo siguiente: ¡en caso de duda, retirar todos los derechos de acceso! Si a consecuencia de esto, un usuario ya no puede acceder a funciones importantes, siempre queda el recurso de concederle esos derechos más tarde, ampliando el correspondiente conjunto de reglas.

Dar de alta y asignar un usuario

Cuando se dispone del conjunto de reglas apropiado para restringir los derechos de un usuario, hay que dar de alta al propio usuario y asignarle el conjunto de reglas. Al apoyarse eSafe en el administrador de usuarios de Windows, el primer paso sería dar de alta al usuario en Windows. Cómo hacerlo ya lo hemos explicado anteriormente en este mismo capítulo. Ahora, para que eSafe reconozca a un usuario conocido en Windows, habrá que darle de alta aquí también.

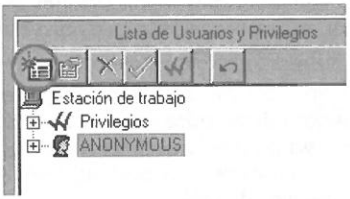
1. Abra en las configuraciones de eSafe la sección *Administración*, pulsando sobre el botón correspondiente.
2. Aquí encontrará las configuraciones del usuario en el registro, en la pestaña *Administración de Usuarios*.

INFO

El usuario anónimo

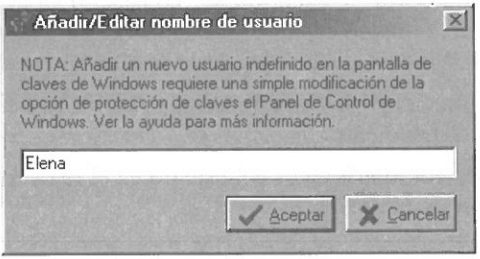
Durante la instalación, eSafe ya dió de alta a un usuario llamado *Anonymous*, es decir, un usuario anónimo. Todo usuario que inicie una sesión en el ordenador y no fuera expresamente registrado como usuario en eSafe con sus propios conjuntos de reglas, recibirá las configuraciones del usuario anónimo. Esto también rige para el caso de que un usuario cancele la ventana de login de Windows, burlando de este modo el procedimiento para registrarse en Windows. El usuario anónimo no puede ser eliminado e incluso cuando se modifiquen sus configuraciones, se recomienda prudencia. Por norma, eSafe asigna al usuario anónimo todos los conjuntos de reglas activados, de modo que sus acciones estarán sujetas a ciertas restricciones. Lo más seguro es definir un conjunto de reglas especial para él, que le retire los permisos de acceso a todos los datos importantes o, según el caso, incluso a todos los datos que usted tenga en el ordenador.

3. Para dar de alta a un nuevo usuario, haga clic dentro del área *Lista de Usuarios y Privilegios* sobre el botón *Nuevo usuario*, situado en el extremo izquierdo.



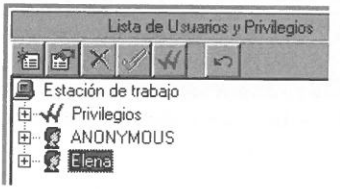
Cree para cada usuario una nueva entrada.

4. En la ventana siguiente *(Añadir/Editar nombre de usuario)*, introduzca el nombre del nuevo usuario. Debe emplear exactamente la misma denominación que éste tenga en el administrador de usuarios de Windows, de lo contrario, cuando el usuario inicie la sesión no será reconocido por eSafe. Confirme la entrada con *Aceptar*.



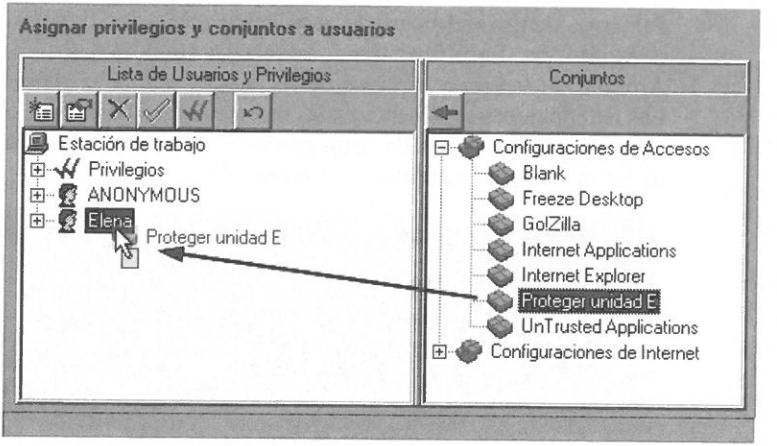
Emplee el mismo nombre de usuario que en el administrador de usuarios de Windows.

5. A continuación, eSafe genera en la lista de usuarios una nueva entrada con el nombre del usuario. Márquelo.



Marque al usuario recién creado, para asignarle sus derechos.

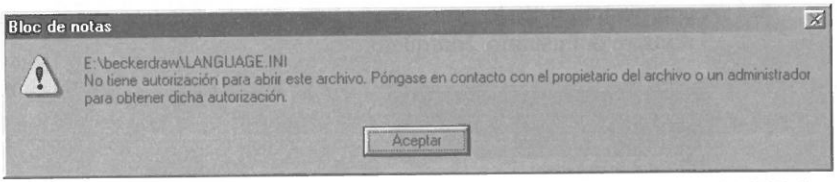
6. Ahora seleccione a la derecha del área *Conjuntos*, debajo del apartado *Configuraciones de Accesos*, el conjunto de reglas que haya definido para ese usuario. Para ello, deberá hacer clic sobre el conjunto de reglas deseado y arrastrarlo con el botón del mouse pulsado hasta el campo de la izquierda. Seleccione el o los conjuntos de reglas y haga clic sobre el botón *Añadir conjuntos*, situado en la parte superior derecha.



De esta forma puede asignar conjuntos de reglas a los usuarios de eSafe.

7. Una vez asignados todos los conjuntos de reglas previstos para el usuario, dé de alta al nuevo usuario, junto a sus restricciones correspondientes, haciendo clic sobre el botón *Aplicar*.

Después, podrá hacer la prueba inciando una sesión con el nombre del usuario recién creado. Intente acceder a los archivos que estén bloqueados para ese usuario. Si los conjuntos de reglas fueron correctamente definidos y asignados, eSafe se lo impedirá. Según la configuración, aparecerá un aviso o un simple mensaje de error de la respectiva aplicación.

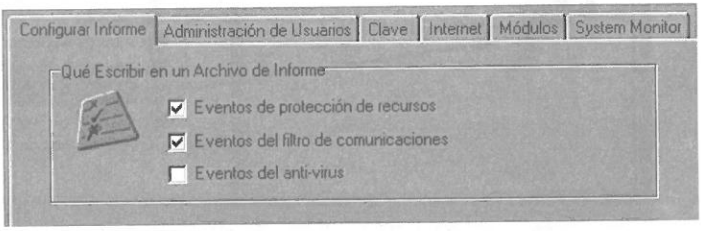


Los accesos que no respeten las reglas definidas serán impedidos con toda fiabilidad por eSafe.

Analizar el protocolo eSafe

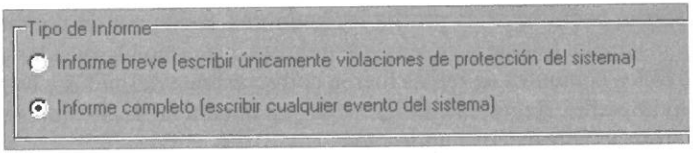
Aparte de las propias funciones de protección, eSafe también le ofrece un mecanismo de control sencillo pero eficaz. El programa registra en un archivo de protocolo todas las violaciones de las reglas, es decir, todas las acciones de usuarios y programas que tuvieron que ser bloqueadas por eSafe obedeciendo a una regla definida previamente.

1. En el programa de configuración de eSafe puede definir en *Configurar Informe*, dentro del apartado *Administración*, los detalles exactos para cada informe. En primer lugar, establezca en el área *Qué escribir en un Archivo de Informe* los tipos de incidencia que deba reflejar el informe. Las tres opciones representan a las tres funciones básicas de eSafe. Pero si, por ejemplo, ya emplea de todos modos otro software antivirus, podrá omitir las incidencias antivirus en el protocolo.



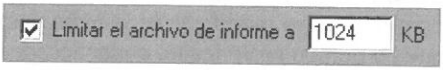
Seleccione en primer lugar los tipos de incidencias que deberá reflejar el informe.

2. Ahora, elija en el área *Tipo de Informe* si quiere recibir un *Informe abreviado* que se concentre en las violaciones de protección, o si prefiere un *Informe completo* que recoja todas las incidencias importantes.



Seleccione tipo y extensión del informe.

3. Para que el archivo de informes no reviente en algún momento los límites de su disco duro, debería delimitar el tamaño máximo del archivo en *Limitar el archivo de informes a X Kb.* Los 1024 KBytes sugeridos por eSafe son un valor absolutamente razonable. Si el archivo alcanza este tamaño, las entradas antiguas serán borradas para hacer sitio a las más recientes.



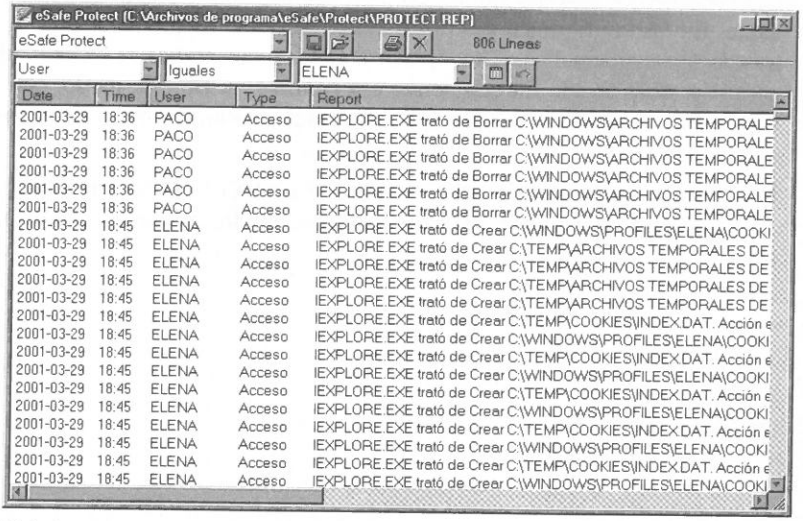
Establezca un límite superior para la extensión de su protocolo.

TRUCO

Configuración correcta del informe

Para obtener un informe útil y bien estructurado, le recomendamos que recoja todos los tipos de violaciones de protección. Es decir, deberá activar las tres primeras opciones. Normalmente, como tipo de informe basta con seleccionar el informe abreviado, que refleja todos los datos importantes. El informe global es muy extenso y confuso, por lo que es fácil pasar por alto informaciones importantes.

Haciendo clic sobre el botón *Ver informe*, situado en la parte inferior, podrá activar el protocolo actualizado. Para cada entrada, eSafe le informará sobre cuándo tuvo lugar la incidencia, qué usuario estuvo implicado, qué tipo de violación de protección sufrió y los recursos a los que afectó. De este modo, usted puede mostrarle al usuario hechos consumados.



El informe de eSafe

2.3 El salvapantallas – una trampa de seguridad

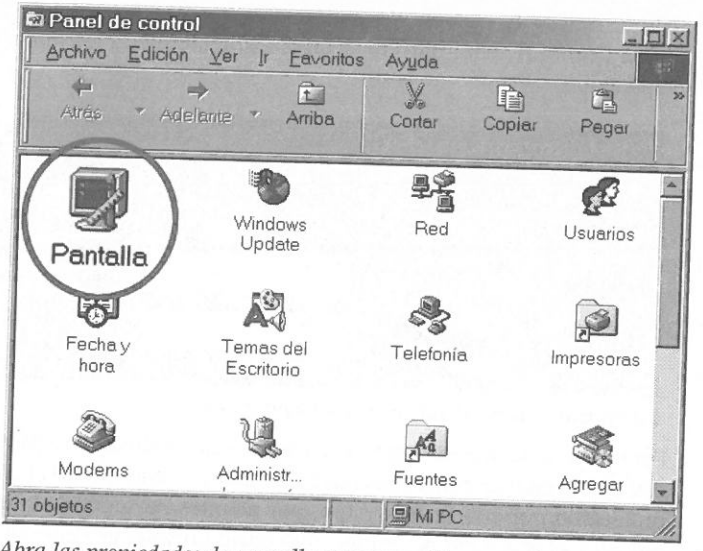
Cuando nos queremos alejar un ratito del ordenador para tomar un café, o simplemente hacer pequeñas gestiones, casi nunca lo desconectamos. ¿Qué puede ocurrir en tan poco tiempo? Pues... muchas cosas. Armado sólo con un disquete o un CD, un intruso hábil podría extraer en un plazo mínimo datos confidenciales de nuestro ordenador, instalar un troyano que más tarde le suministre contraseñas y otra información confidencial, o modificar su sistema para más adelante, si nos ausentamos durante un tiempo prolongado, poder acceder a todo el sistema. El mejor concepto de seguridad con contraseñas BIOS y un administrador de usuarios eficaz, se queda en nada si el agresor puede apoderarse sin más de nuestro PC durante un descuido.

Un recurso popular para mantener ocupados los PCs durante pausas y ausencias breves, son los salvapantallas. Se conectan automáticamente tras determinado tiempo de inactividad en el ordenador. Originalmente su finalidad era proteger el monitor del PC para que una imagen que haya estado quieta durante mucho tiempo, no quede fijada para siempre dentro del tubo de imagen. Este peligro se daba en los monitores antiguos. Con los aparatos modernos, ya no puede ocurrir algo así. Hoy en día, mucha gente ve en el salvapantallas más un pasatiempo del tipo "¡Mira, qué guay es mi salvapantallas nuevo!"

Preparar el salvapantallas con contraseña

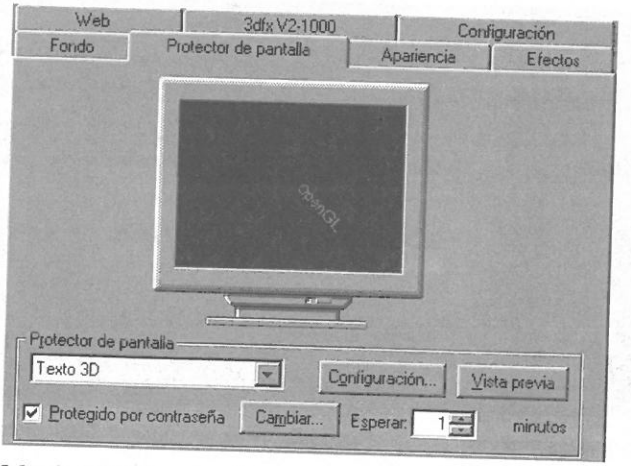
Ciertamente, los salvapantallas cumplen una función de seguridad nada desdeñable. En las configuraciones del sistema Windows se puede asignar una contraseña al salvapantallas. Esto significa: si el salvapantallas se ha activado, sólo podrá ser desactivado introduciendo esa contraseña. De este modo, con un salvapantallas se puede proteger al PC de accesos no autorizados durante ausencias cortas.

1. Abra la configuración del sistema con *Inicio/Configuración/Panel de control* y una vez dentro, abra con un doble clic las propiedades de pantalla.



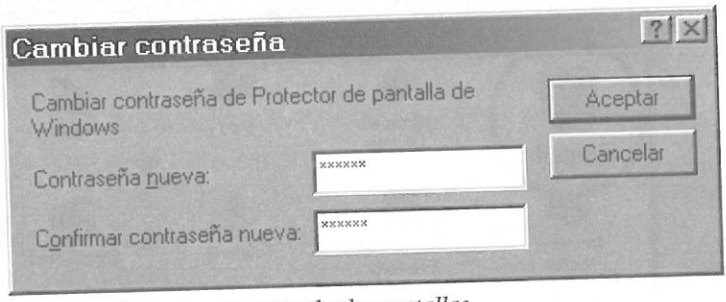
Abra las propiedades de pantalla para especificar un salvapantallas.

2. Cambie ahora a la categoría *Protector de pantalla*.
3. Si aún no tenía ningún salvapantallas activo, elija uno de los que se ofrecen en la lista de selección. En el monitor simbólico que aparece en la ventana, verá una muestra del salvapantallas que acaba de marcar. Haciendo clic sobre el botón *Configuración* podrá configurar la mayoría de los salvapantallas con más detalle.



Seleccione el salvapantallas y active la protección por contraseña.

4. Ahora, active la opción *Protegido por contraseña* y haga clic sobre el botón *Cambiar*, para introducir en el siguiente menú la contraseña del salvapantallas.

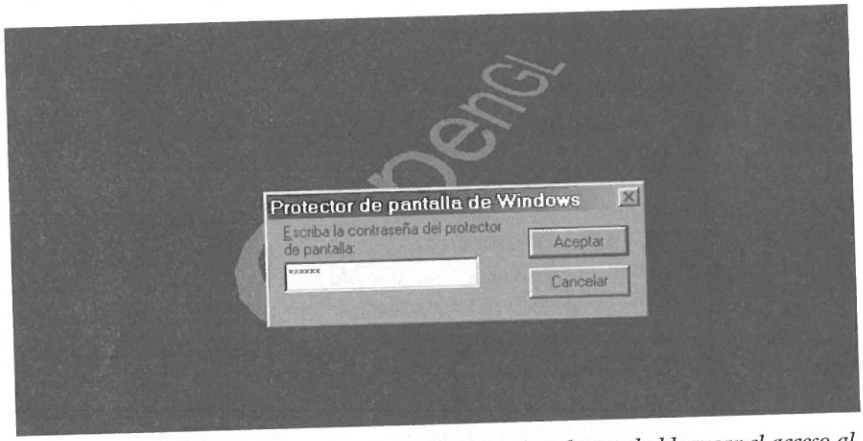


Introduzca la contraseña para el salvapantallas.

5. Finalmente, dentro del campo *Esperar* podrá indicar el tiempo de inactividad tras el cual deberá conectarse automáticamente el salvapantallas con su protección por contraseña. Aquí, por razones de seguridad, le recomiendo que elija el intervalo de tiempo más corto posible, es decir, un minuto.

6. Confirme los nuevos ajustes con *Aceptar*.

Desde ahora, el salvapantallas se activará automáticamente en cuanto haya transcurrido cierto tiempo de inactividad por parte del usuario. En este caso, vuelva al ordenador y "despiértele". Aunque, en este caso, ya no volverá a la normalidad sin más. Le pedirá la contraseña. Sólo si la introduce correctamente podrá seguir trabajando.



El salvapantallas pregunta por la contraseña antes de volver a desbloquear el acceso al ordenador.

TRUCO

Activar el salvapantallas manualmente

Un problema del salvapantallas es, que sólo se activa automáticamente tras haber transcurrido el tiempo de inactividad que se definiera previamente. Tendría más sentido si pudiera ser activado directamente cada vez que fuera necesario, es decir, cuando el usuario quisiera alejarse un rato del ordenador. Aunque esto puede hacerse utilizando un pequeño truco: cree en el escritorio de Windows un acceso directo a su salvapantallas. Para ello, debe abrir con el Explorador la carpeta C:*Windows**System*. Aquí encontrará todos los archivos de salvapantallas, cuyos nombres acaban en *.scr*. Haga clic sobre el archivo de su salvapantallas preferido y arrastre su icono con el mouse al lugar deseado del escritorio. Windows creará allí un acceso directo al archivo del salvapantallas, que usted podrá activar desde ahora manualmente con un doble clic. La configuración se seguirá realizando a través de las *Propiedades de Pantalla* en el panel de control.

Así de segura es la contraseña del salvapantallas

El mecanismo del salvapantallas de Windows es relativamente seguro. Así, cuando se introduce la contraseña para la reactivación, queda desactivada toda posibilidad de burlar la petición de contraseña, como por ejemplo la combinación de teclas para la lista de tareas. Por lo tanto, con simples trucos caseros no se consigue nada. Aunque al agresor siempre le queda la posibilidad de desconectar el ordenador sin más. Sólo si el arranque del PC había sido protegido también por una contraseña BIOS, tendrá sentido emplear un salvapantallas con contraseña. Además, hay programas especiales que permiten burlar a los salvapantallas que no dispongan de dispositivos de protección especiales, aunque tengan contraseña. El funcionamiento de estos programas queda muy bien demostrado por *Screen Saver Destroyer 2000*, del que podrá descargar una versión de prueba gratuita en la dirección: http://www.the-hitman.com/wtm/. Esta versión de prueba gratuita está "descafeinada" y sólo funcionará, si usted arranca el programa antes de que se haya activado el salvapantallas. La versión completa cuesta $ 40 y viene en un CD-ROM especial, que se puede insertar en un PC con salvapantallas activo para burlarle.

El Screen Saver Destroyer consiste en un pequeño programa que funciona en paralelo con el salvapantallas y cuya ventana puede ser visualizada y utilizada a pesar de éste.

La ventana de programa del Screen Saver Destroyer se impone al salvapantallas.

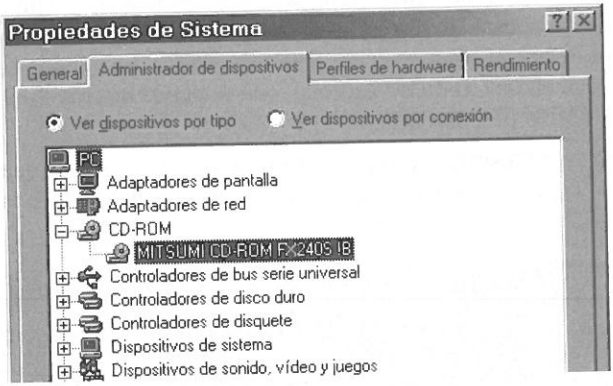
Si el salvapantallas está activo, usted sólo tendrá que hacer clic sobre el botón *Detect*. Entonces, el programa buscará el salvapantallas activo en la memoria de trabajo del ordenador. Si lo encuentra, visualizará su nombre. Al mismo tiempo liberará el botón *Kill*. Si usted hace clic sobre éste, podrá "liquidar" al salvapantallas y acceder al ordenador sin necesidad de introducir la contraseña.

Una vez detectado el salvapantallas, se le puede echar de la memoria con un simple clic del mouse.

Protección contra el destructor de pantallas

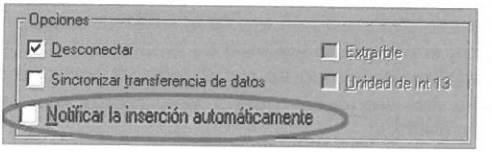
Los programas para burlar un salvapantallas siempre se aprovechan de los agujeros de seguridad. El principio funcional de la versión íntegra del Screen Saver Destroyer se basa en que al insertar un nuevo CD, Windows siempre intenta arrancarlo automáticamente, o reproducirlo si se trata de un CD Audio. Esto también ocurre estando activado el salvapantallas. Es decir, el CD del Screen Saver Destroyer ha sido diseñado para que el programa sea arrancado automáticamente nada más insertar el CD. Este agujero de seguridad puede ser cerrado si se evita la reproducción automática de los CDs. Con este fin, se puede cambiar una opción en las profundidades de la configuración de Windows.

1. Abra el panel de control y dentro de éste, seleccione *Sistema*.
2. Ahora, cambie a la categoría *Administrador de dispositivos* y busque en la lista de dispositivos la entrada *CD-ROM*.



Abra las configuraciones para su(s) unidad(es) de CD-ROM.

3. Con un doble clic sobre la entrada del disco abrirá las propiedades para este dispositivo. En la categoría Opciones podrá desactivar la casilla *Notificar la inserción automáticamente*. Esta es la responsable de que el sistema operativo reaccione cuando cambie el CD.



Esta opción controla el comportamiento del sistema operativo cuando cambia el CD.

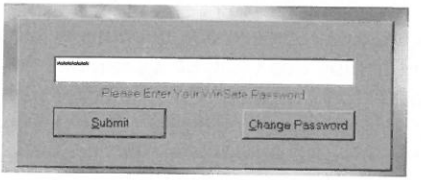
4. Si dispone de varias unidades de CD-ROM o de una grabadora de CDs adicional, tendrá que repetir este ajuste para cada una de ellas.

5. A continuación, haga doble clic sobre *Aceptar* para actualizar las nuevas configuraciones, que no serán operativas hasta que vuelva a arrancar el PC.

Con esto, ya ha tapado este agujero de seguridad de Windows. Sin embargo, tendrá que renunciar a la comodidad de que los CDs arranquen automáticamente nada más ser insertados en su unidad, o de que la reproducción de CDs de audio comience automáticamente. Desgraciadamente, ese el precio que exige la seguridad.

Salvapantallas seguros

Otra posibilidad es emplear un salvapantallas que haya sido diseñado especialmente para la protección de acceso. Estos programas también llevan protección por contraseña, pero no pueden ser desterrados de la memoria de trabajo con tanta facilidad. Además, van un poco más lejos que los salvapantallas normales de Windows y, por ejemplo, bloquean todas las funciones que no se requieran directamente para la introducción de la contraseña. Así ya no se pueden emplear programas como Screen Saver Destroyer, por poner un ejemplo. Un vigilante fiable de este tipo es el programa *WinSafe*. Usted se puede bajar una versión prueba desde http://www.ruzzy.co.uk. WinSafe es un programa autónomo, por lo que los programas killer no lo reconocen como típico salvapantallas. También puede ser empleado adicionalmente durante el inicio de sesión en Windows, para hermetizarlo completamente.



WinSafe es un salvapantallas nada fácil de forzar.

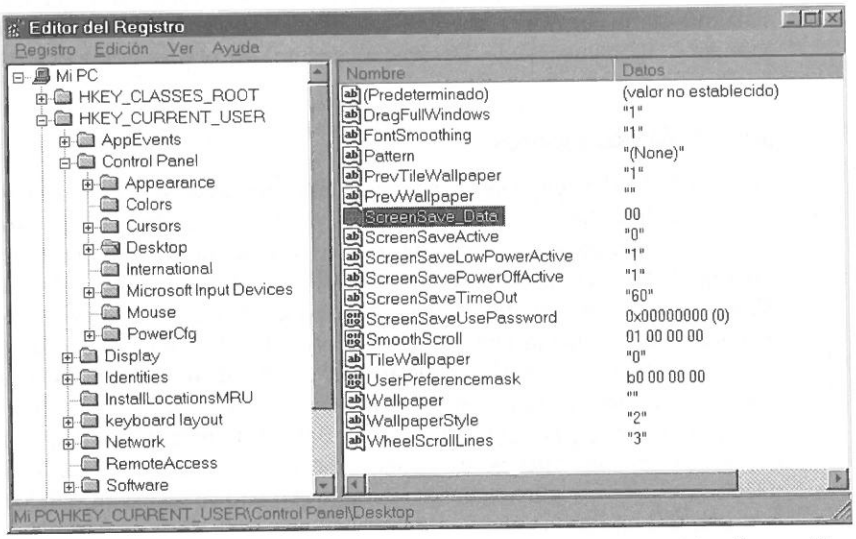
TRUCO

Cualquier programa como salvapantallas

Si quiere emplear WinSafe u otros programas como salvapantallas, no es imprescindible que los arranque manualmente. En realidad, la función de salvapantallas de Windows es capaz de arrancar cualquier programa. Usted sólo lo tiene que copiar a la carpeta *C:\Windows\System*, donde también están guardados los salvapantallas. Cambie el sufijo de programa *.exe* a *.scr*. A continuación, el programa figurará en la selección de las configuraciones de salvapantallas, donde podrá ser elegido. A partir de ahora, Windows arrancará este programa cuando haya expirado el tiempo de inactividad previamente definido.

La contraseña del salvapantallas

Por desgracia, la contraseña del salvapantallas de Windows no está lo suficientemente protegida. Windows la guarda en la base de datos de registro. Allí no estará en texto claro, pero el método de cifrado no es demasiado complicado. Los hackers disponen de programas, con los que pueden descodificar estos datos sin mayor dificultad y averiguar la contraseña.



La contraseña del salvapantallas se guarda en el registro con una codificación sencilla.

Desde el punto de vista de seguridad, esto significa que mientras el salvapantallas esté realmente activado todo el tiempo que usted se ausente del ordenador, podrá confiar en él. Pero, si a pesar de todo, alguien consigue echar mano de su PC durante su ausencia, podrá espiar la contraseña y burlar a la petición de contraseña. En consecuencia, sólo deberíamos ausentarnos del PC cuando esté acti-

vado el salvapantallas o el ordenador esté desconectado. Además, para ir sobre seguro, también es recomendable cambiar con regularidad la contraseña del salvapantallas

2.4 Protección por contraseña para el PC y los datos

La seguridad comienza ya al conectar el ordenador. Desde este momento, nada más arrancar el PC o iniciar Windows, tendremos los primeros puntos de ataque para el hacker que quiera acceder a su ordenador. Estos puntos críticos deberían ser protegidos por contraseña. En este apartado vamos a contarles todo sobre cómo deben ser las contraseñas seguras, dónde pueden ser empleadas, hasta qué punto son fiables y cómo protegerse de ataques sobre las mismas.

INFO

Cuantiosos daños debido al robo de una contraseña

Una noticia que en los últimos tiempos se puede leer cada vez con mayor frecuencia. El 14 de diciembre de 2000, PC World hizo el siguiente aviso: *¡40 internautas hacen uso indebido de contraseñas!*

La historia se cuenta pronto. Un usuario incauto había guardado en el PC su identificador de Internet junto a su contraseña correspondiente. Hackers desconocidos consiguieron robar esta información con la ayuda de un troyano. Publicaron los datos robados en Internet, donde fueron hallados por 40 internautas que navegaron por la Red a costa de la víctima. En total, causaron pérdidas por un valor aproximado de 4.000.000 de Ptas. Y una nueva cita extraída de la noticia: "Los usuarios de Internet deben evitar a toda costa guardar sus contraseñas en el ordenador por comodidad", advirtió la Policía.

La importancia de las contraseñas

Proteger datos quiere decir, impedir por norma todo acceso y hacer excepciones sólo con determinados usuarios autorizados. Si pretende que el ordenador sepa que usted es uno de estos usuarios autorizados, deberá identificarse ante él. Para lo cual necesitará normalmente dos cosas:

- Un identificador de usuario por el cual le reconocerá el ordenador. Basándose en ese nombre, le permitirá acceder a determinados datos y recursos. El nombre de usuario se emplea, además, para recoger sus actividades en un registro y, por ejemplo, en un servicio online facturarlas. El identificador de usuario es asignado en la mayoría de los casos por el operador del ordenador o de la red. No es necesario mantenerlo en secreto. Por el contrario, en las comunicaciones por correo electrónico forma parte imprescindible de la dirección.

- Cada nombre de usuario tiene su correspondiente contraseña. Esta palabra clave secreta es algo así como una llave. Por el hecho de conocerla, usted demuestra al ordenador cuando inicia la sesión, que es realmente quien dice ser.

Por lo tanto la contraseña es, junto con su nombre de usuario, el ticket de entrada a todo lo que tenga que ver con datos confidenciales y personales. No sólo su propio ordenador podrá ser protegido de este modo. También para acceder a Internet, el servicio online le exigirá a usted una contraseña cuando inicie la sesión. Del mismo modo tendrá que registrarse en la Banca Electrónica e identificarse antes de recibir acceso a su cuenta. Por un lado, esto significa que le conviene no olvidarse de su contraseña, para no excluirse a sí mismo del acceso a sus datos y las posibilidades de comunicación. Pero, por el otro, también implica que cualquiera que conozca su contraseña puede servirse en su nombre de estos datos y accesos.

¿Qué está en juego?

Cualquiera que se apropie de su contraseña podrá hacer en el ordenador y en la respectiva red todo aquello para lo que usted esté autorizado y perpetrar acciones que usted nunca haría. Si por ejemplo, alguien le robara su acceso online, podría navegar por la Red a costa de usted. Cuando se aburriera, podría asumir su identidad. Figúrese que participara con su nombre en canales de chat u otros foros online. Y ahora, piense por un momento en la peor fechoría qué pudiera cometer allí esa persona.

Además, de paso podría excluirle a usted de sus accesos y datos cambiando la contraseña, de modo que usted ya no podría acceder. Si es cliente de un proveedor de servicios online de pago o incluso banca, como Terra Profesional o Patagon, aún podría ser peor. Estos proveedores ofrecen costosos servicios adicionales, de los que el ladrón podría hacer uso. Todos los servicios adicionales, pedidos y otros costes aparecerán en su factura mensual. Aún en el caso de que pudiera demostrar el uso fraudulento de sus datos de acceso por otra persona, el proveedor de servicios online le cobraría a usted.

Si posee en la Red su propia página web protegida por la contraseña robada, el intruso podría llegar a ser muy creativo. Lo de menos sería que le desfigurara sus páginas. ¿Quién sabe si no las emplearía para difundir contenidos ilegales con su nombre?

Hay multitud de posibilidades que pueden ser reducidas fácilmente a un denominador común: si alguien conoce su contraseña, podrá costarle su reputación, su acceso online y mucho dinero. Sin contar con que tendría acceso a sus datos más personales y delicados.

Así son seguras las contraseñas

Una protección eficaz por contraseña comienza con la elección de la misma. Una contraseña que pueda ser adivinada con facilidad por los demás, equivale a no tener ninguna. Por eso, gran parte de conceptos próximos a nuestro entorno no sirven como contraseña:

- nuestro nombre, al igual que el de esposas, novias, hijos o mascotas,
- nuestro color preferido, nuestra cinta favorita, el autor predilecto u otras preferencias...
- la marca, el tipo o la matrícula de nuestro automóvil,
- nuestra fecha de nacimiento, la de parientes o amigos,
- el código postal o nombre de nuestro lugar de residencia,
- al igual que todos los conceptos que cualquiera pueda saber o averiguar, aunque nos conozca muy poco.

Incluso si elige conceptos menos relacionados con su entorno, debería procurar no emplear palabras según figuren, por ejemplo, en enciclopedias o diccionarios. Son precisamente esas listas de palabras las que emplean los hackers para averiguar una contraseña por las bravas. Por eso, toda contraseña debería incluir elementos que con absoluta seguridad no figuren en ningún diccionario. Una buena regla es insertar en cada contraseña al menos un número y un signo especial (por ejemplo . ,;:_?!+-&$§), que podrían ir en cualquier posición. Combinando estos elementos con una palabra sencilla de memorizar, podemos componer una contraseña más o menos fácil de recordar.

TRUCO

La frase personal

¿Busca usted una contraseña fácil de recordar que además sea segura? Entonces invente simplemente una frase muy personal, de la que pueda acordarse sin problemas. Por ejemplo: "*De niño tuve un gato llamado Félix*" Si ahora, usted coge la primera letra (o también la segunda, la tercera, la última, etc.) de cada palabra, obtendrá una estupenda contraseña. En este caso, sería *DntuglF*. Una palabra que parece carecer de significado y jamás aparecerá en ninguna enciclopedia. A pesar de todo, para usted esta combinación exótica tiene sentido y la podrá recordar con facilidad.

Si los números y signos especiales le parecen demasiado difíciles de recordar, hay un truco que cumple la misma finalidad casi igual de bien. Coja una palabra normal y corriente que no se refiera demasiado a su entorno personal, pero que usted pueda recordar con facilidad. Introduzca a sabiendas un error de ortografía en esa palabra. Por ejemplo *Belrin* en lugar de *Berlín*. Esto también sirve para protegerle ampliamente de un ataque con listas de palabras.

¿Qué longitud debería tener una buena contraseña?

La respuesta a esta pregunta parece obvia: cuanto más larga, mejor. Pero en la realidad, esto no es tan sencillo. Naturalmente, desde el punto de vista técnico, la seguridad de una contraseña depende de su longitud. Una contraseña de sólo un signo podrá ser adivinada por cualquiera en poco tiempo, mediante el sencillo procedimiento de hacer pruebas. Todo signo que se le añada, elevará el esfuerzo necesario para descifrarla, de modo que una contraseña de diez dígitos será difícil de desencriptar aún empleando recursos técnicos.

INFO

Limitaciones de longitud

A veces, la longitud de la contraseña no sólo depende de lo que usted elija. Algunas aplicaciones exigen una longitud determinada. El ejemplo más conocido pueden ser los PINs de las tarjetas bancarias, que por norma tienen cuatro dígitos. Lo mismo ocurre con otras aplicaciones PIN, como p.ej. la banca electrónica online, donde los números secretos casi siempre pueden ocupar sólo de cuatro a seis dígitos. Por regla general, estas limitaciones tienen su causa en el software empleado, que dispone de un espacio de memoria restringido para procesar los PINs. También a la hora de elegir contraseñas hay unas longitudes mínimas. Seguramente, ya le informarán a usted antes de introducir por primera vez una contraseña, aunque en algunos casos, no se enterará hasta después de haber elegido una contraseña demasiado corta y haber sido advertido por el programa. Pero en este caso, él le informará a usted de la longitud que debe tener la contraseña. Si bien puede resultar algo enervante tener que hacer un sinfín de intentos para encontrar la contraseña apropiada, los sistemas que verifican la seguridad de las contraseñas introducidas por el usuario resultan muy útiles. Ayudan al usuario a evitar los errores más frecuentes al elegir contraseñas seguras.

Pero los hackers no se limitan a emplear recursos técnicos. Un método tan sencillo como eficaz es espiar a la víctima mientras teclea su palabra clave. Si su contraseña es tan larga y complicada que usted la tiene que teclear muy despacio y, aun así, se equivoca y se ve obligado introducirla otra vez, dará al mirón todo tipo de oportunidades para ver al menos algunas partes del concepto buscado. Si es capaz de deducir el resto, ya habrá quedado al descubierto su contraseña. Por lo tanto, cuando la elija procure que no sólo sea segura, sino también que pueda ser tecleada rápida y fluidamente.

Si quiere ir a lo seguro y, además, tiene buena memoria, hay un método relativamente sencillo para inventarse contraseñas muy fiables. Cierre los ojos y pulse el teclado varias veces con diferentes dedos. Compruebe el resultado y, si lo desea, añada algunos números y símbolos especiales. Si consigue grabárselo en la memoria, tendrá una contraseña que nadie podrá adivinar.

TRUCO

El empleo de mayúsculas y minúsculas en las contraseñas

En cuanto al empleo de mayúsculas y minúsculas en las contraseñas, hay que tener en cuenta fundamentalmente dos técnicas diferentes. En los PCs, los sistemas operativos de Windows no distinguen entre letras mayúsculas y minúsculas. Es decir, *Gelb1?* será reconocido como contraseña correcta igual que *gelb1?*. Esto cambia en los grandes ordenadores Unix y en los PCs con Linux. Distinguen las letras mayúsculas y minúsculas como dos modos de escritura diferentes. Por lo tanto, *Gelb1?* no equivaldrá a *gelb1?*. Asimismo, como usuario de PC podría toparse con problemas de este tipo, si por ejemplo se conecta a uno de estos ordenadores Unix a través de Internet o una red local. Si le ocurriera algo así, compruebe en primer lugar si ha escrito correctamente las mayúsculas y minúsculas de la contraseña.

Proteger las contraseñas

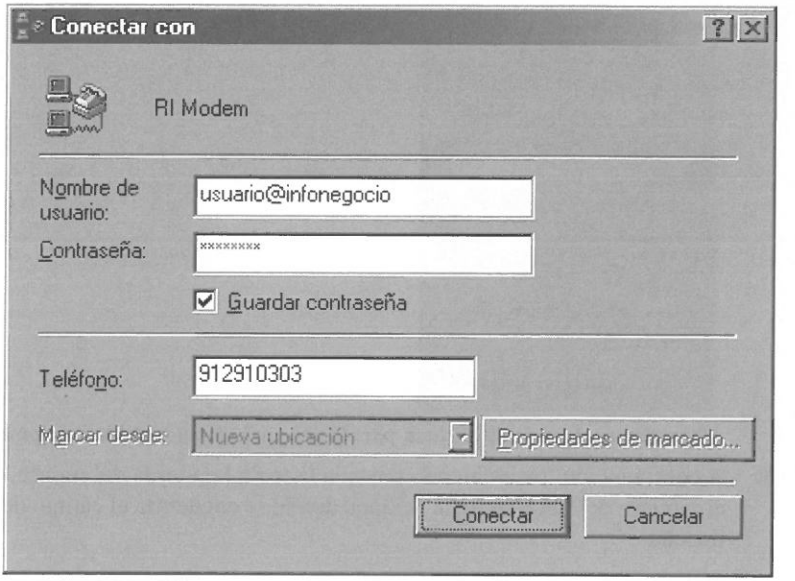
Hasta una contraseña elegida con agudeza dista mucho de ser segura. Para que sea realmente secreta, debería tratarla con el mismo cuidado que a su número secreto de la tarjeta bancaria, o como si fuera la combinación de una caja fuerte. Esto implica guardar la contraseña exclusivamente en la propia memoria, no dejarla por escrito en ninguna parte y no decírsela a nadie. Aparte de esto, hay una serie de medidas especiales de precaución para manejar las contraseñas.

- Cuando le dan un nuevo acceso de usuario, éste suele constar de un identificador de usuario y una contraseña generada automáticamente. En la mayoría de los casos, esto se hace siguiendo reglas sencillas, por ejemplo en función del identificador de usuario o de la fecha de registro. También los hackers conocen estas reglas y peinan con frecuencia los sistemas para detectar a estos nuevos usuarios. Por tanto, nada más recibir sus datos de acceso haga login y cambie su contraseña.
- Algunos proveedores de redes desisten totalmente de emplear una contraseña inicial. Aquí, el acceso estará sin protección hasta que el usuario haga su primer login. Entonces, se le pedirá automáticamente que introduzca una contraseña. Pero, quién dice que ese acceso libre no podrá ser detectado por un hacker y se apropie de él. También, por este motivo, se recomienda no perder tiempo en el primer login de un nuevo acceso.
- Jamás escriba su contraseña en un archivo, ni la fije al monitor con una nota adhesiva. Asimismo, lo de esconderla bajo la carpeta ya es de sobra conocido por las películas de James Bond. Además, nunca fue seguro. Salvo que usted viva como ermitaño en una isla desierta, deberá hacerse a la idea de que otras personas pueden acceder a su escritorio y a su ordenador, apropiándose de estos escondites. Si quiere guardar sus contraseñas en el ordenador, emplee un programa que las archive codificadas (consulte al respecto el apartado sobre los programas para administrar contraseñas, que viene más adelante).

- Nunca ceda su contraseña a otra persona, por mucho que confíe en ella. Aunque ésta no haga un uso fraudulento de la misma, podría revelársela a otros por descuido. "Prestar" la contraseña significa siempre, ceder el control sobre ella. Tampoco los empleados de su proveedor de redes preguntan jamás a un cliente por su contraseña. Aunque este es un truco muy apreciado entre los hackers.
- Si a pesar de todo, en algún momento se viera obligado a comunicar su contraseña a otra persona, proceda de la siguiente manera: cambie primero la contraseña actual por otra. Esta nueva clave secreta debería ser absolutamente neutra y no revelar al otro el modo en que usted concibe su contraseña. Dígasela al otro y aclárele hasta cuándo podrá utilizar su acceso. En cuanto expire este plazo, haga login y vuelva a cambiar la clave secreta. Podrá volver a introducir la anterior, o aprovechar la ocasión para hacer un cambio.
- La regla más importante es: cambie regularmente su contraseña, aunque resulte incómodo. Nunca se puede saber si pese a todas las precauciones, alguien ha podido espiar o desencriptar nuestra clave secreta. Cuando nos damos cuenta, casi siempre es demasiado tarde y el daño ya está hecho. Pero si cambia su contraseña con regularidad, dejará al intruso muy poco tiempo para hacer daño con el acceso hurtado. A fin de cuentas, ahora tendrá que averiguar la nueva contraseña. Si un hacker le ha elegido a usted como objetivo, un cambio regular de la contraseña podría espantarle.

Peligro: guardar las contraseñas en los diálogos de inicio de sesión

Muchos programas de login y acceso ofrecen la posibilidad de guardar datos de acceso, como el nombre de usuario y la contraseña. Esto exime al usuario de la molesta obligación de teclear siempre lo mismo. Desde luego, resulta muy cómodo. Pero es de todo menos seguro. Imagine que roban en su casa y se llevan su ordenador. Si el ladrón puede acceder a él sin necesidad de introducir contraseña y puede activar su acceso a Internet, por ejemplo, no hará falta que sea un hacker para que navegue a su costa por toda la Red. En resumen, grabar una contraseña para establecer la conexión automáticamente es lo mismo que no tener ninguna. Aunque otro no pueda leerla (porque no es visualizada en texto claro), podrá procurarse el acceso cuando quiera.



Tentadoramente cómodo, pero muy inseguro: diálogos con contraseñas guardadas.

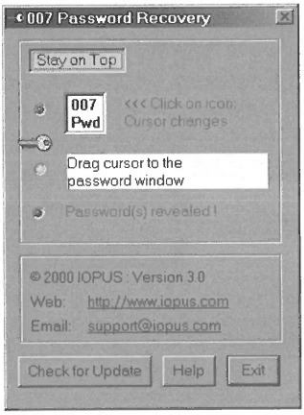
Otra razón por la que no se debería guardar la contraseña en los cuadros de diálogo de inicio de sesión: los asteriscos (***) que la ocultan no dejan de ser un simple escondrijo. Empleando el software adecuado, es posible eliminarlos y visualizar en su lugar la contraseña real. Si le cuesta creerlo, ¿por qué no hace la prueba? Con el programa *007 Password Recovery*, que puede descargar gratis desde http://www.iopus.com, podrá verificar hasta qué punto son seguros los diálogos de contraseña en sus aplicaciones. Si un diálogo no supera el siguiente test, más vale que jamás guarde en él la contraseña.

TRUCO

¿Ha olvidado la contraseña?

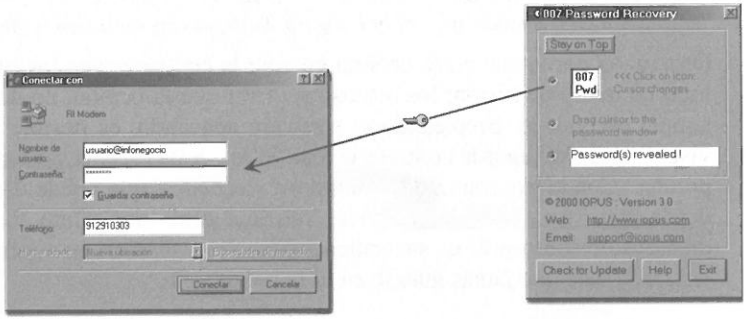
007 Password Recovery no sólo sirve de ayuda a la hora de hacer tests de seguridad. Su función verdadera es ayudar a los usuarios que en algún momento guardaron su contraseña, desde entonces la utilizaban siempre automáticamente, pero de repente y ante una situación concreta, no conseguían recordarla. ¡Naturalmente, este programa no ha sido concebido para espiar contraseñas ajenas!

1. Usted podrá arrancar este programa siempre que aparezca un diálogo con una contraseña guardada.
2. Entonces, haga clic con la tecla izquierda del mouse sobre el botón de la clave y mantenga pulsada esta tecla. El puntero del mouse se convertirá en el símbolo de una llave.



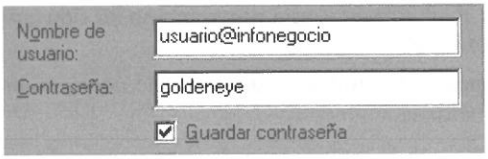
Haga clic en el botón de la clave, para arrancar la función de desencriptación.

3. A continuación, manteniendo pulsada la tecla izquierda del mouse, arrastre el puntero del ratón hasta la ventana donde se encuentra el campo de la contraseña.



Arrastre el símbolo de la llave hasta el interior de la ventana donde esté la contraseña que pretenda desencriptar.

4. Conforme vaya arrastrando el símbolo sobre la ventana de la contraseña, aparecerá en texto claro la palabra clave oculta.



Ahora se puede ver la contraseña que originalmente estaba oculta.

De este modo, usted puede hacer visibles todas las contraseñas en todas las aplicaciones que empleen funciones estándar de Windows. Los programas realmente seguros aplican aquí sus propias funciones que no se dejan embaucar tan fácilmente, aunque esto suele ser más bien la excepción. Actuando según lo descrito, los ladrones de contraseñas pueden hacerse con las palabras clave ajenas, anotarlas y emplearlas en cualquier otro ordenador, por ejemplo, si quieren conectarse a Internet o a un servicio online.

INFO

¿Autocompletar?

Los actuales navegadores web disponen de numerosas funciones, cuya finalidad es facilitar al máximo a los usuarios su navegación por la red. Incluyen también las funciones de autocompletar, que sirven para rellenar automáticamente con los datos correctos las páginas de formularios a las que se acceda regularmente. También en este caso, la comodidad supone una considerable merma de seguridad. Si por ejemplo, puede registrarse en una oferta web confidencial sin necesidad de introducir ninguna contraseña, porque el propio navegador se encarga de ello, también podrá hacerlo cualquier otra persona que consiga acceso a su ordenador. Por lo que jamás se debería recurrir a la función de Autocompletar para el PIN de banca electrónica. En los datos menos confidenciales, puede permitir que sean rellenados automáticamente. Para eso resulta especialmente recomendable Netscape Navigator (a partir de la versión 6.0), ya que su función de Autocompletar está protegida por una contraseña propia.

Síntomas de que la contraseña ha sido pirateada

Mientras un ladrón de contraseña no haga algo realmente llamativo – como por ejemplo modificar la contraseña antigua – usted, seguramente, no se percatará de su presencia hasta que sea demasiado tarde. Es decir, cuando la factura del proveedor de servicios online le provoque un desmayo, o le caigan encima otro tipo de sorpresas desagradables. Pero hay algunas señales a las que podría estar atento.

- Si de repente, recibe multitud de correos electrónicos raros, que se refieren a temas totalmente extraños o proceden de un remitente absolutamente desconocido. Quizá el ladrón de la contraseña se esté comunicando con su nombre.
- Si usted quiere conectarse a Internet o a su proveedor de servicios online y es rechazado con un mensaje de error, que le advierte de que ya está conectado. Esto puede deberse también a un error de su proveedor de servicios. Pero si estos incidentes se acumulan, debería investigarlos sin falta.
- También puede ocurrir que su proveedor de servicios le haya amonestado por sus frecuentes conexiones múltiples. En este caso, significará que un intruso está conectado al mismo tiempo con la identidad de usted. Pero el

proveedor piensa que es usted quien se ha conectado varias veces y está molesto.

- Vigile si en grupos de noticias u otros foros de noticias similares aparecen contribuciones presuntamente redactadas por usted. También suponen advertencias inequívocas las respuestas a esta clase de artículos o las observaciones de conocidos virtuales sobre sus actividades.
- Si su proveedor de servicios online advierte que alguien se equivoca frecuentemente en el intento de iniciar una sesión con su identificador de usuario. En realidad, los operadores de sistemas deberían darse cuenta por sí mismos de que alguien está haciendo algo ilícito. Pero les gusta atribuir los problemas de funcionamiento a la ineptitud de los clientes. Si su proveedor le amonestara con frecuencia por incidentes de este tipo, déjele inmediatamente claro que usted no es el causante. Insista sobre todo en que aclare estas incidencias.
- Compruebe regularmente sus datos online, como el buzón de correo electrónico o los archivos, para ver si presentan cambios llamativos. Aunque generalmente los hackers se esfuercen en borrar todas sus huellas, quizá puedan delatarse por algún descuido.

Medidas inmediatas

Lo ideal sería que nadie supiera jamás su contraseña, sobre todo si usted tiene en cuenta las reglas que hemos explicado en las páginas precedentes. Si pese a todo, le llegaran advertencias o pruebas concretas de que alguien está utilizando su contraseña ilícitamente, hay algunas acciones que debería emprender inmediatamente:

1. Si es posible cambie su contraseña enseguida, procurando ante todo que sea segura. Ya hemos explicado al comienzo de este capítulo cómo debería ser esa contraseña.
2. Si usted ya no puede iniciar la sesión por haber cambiado el intruso la contraseña, póngase en contacto inmediatamente con su proveedor de redes. Descríbale lo ocurrido. Solicite al administrador que cambie la contraseña o, según el caso, bloquee totalmente el acceso. Cuanto antes lo haga, mucho mejor. Tenga en cuenta que el intruso puede ocasionarle sin parar costes que repercutirán en su factura de servicios online, o también cualquier otro daño.
3. Aunque usted mismo pueda cambiar la contraseña, debería comunicar el incidente inmediatamente a su proveedor de redes. Quizá el hacker no sólo se haya colado en su acceso. Además, sólo así podrá quedarle una oportunidad de no tener que pagar los costes adicionales que puedan originarse.

4. Verifique los foros y grupos de noticias, para ver si figuran noticias enviadas con su dirección. Si las encuentra, informe al correspondiente grupo de que su contraseña ha sido utilizada ilícitamente y deje claro que esa noticia no era suya.
5. Si posee un acceso online con buzón de correo electrónico (p.ej. AOL), verifique los mensajes enviados y los recibidos. Vigile durante un tiempo si entran mensajes insólitos. Aclare la situación, si fuera necesario.
6. Durante el tiempo posterior, cambie su contraseña con frecuencia. Puede ser que el intruso intente hacerse de nuevo con sus datos de usuario. Pero si advierte que usted ha detectado el peligro y se ha enfrentado a él, perderá pronto el interés.
7. Insista a su proveedor de redes, para que haga todo lo que esté en sus manos por aclarar estas incidencias y descubrir al malhechor. Sólo así podrá estar seguro de que en el futuro le deje en paz. Además, de este modo tendrá un culpable para posibles demandas de daños y perjuicios.
8. Si usted fuera repetidamente víctima de un hacker, solicite que desactiven su acceso y le creen uno completamente nuevo. Si fuera necesario, cambie también de proveedor de redes o haga que registren el nuevo acceso en el sistema bajo otro nombre. Así, podrá despistar también a los "enemigos íntimos".

Contraseñas en aplicaciones y documentos

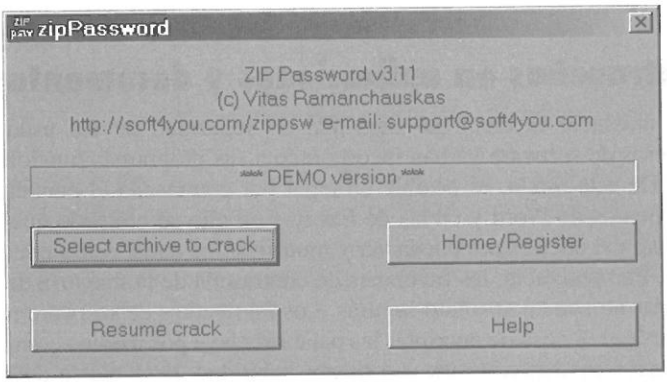
Para satisfacer la creciente demanda de seguridad de los usuarios, algunas empresas de software ya han incorporado a sus programas funciones de protección. De este modo, es posible proteger por contraseña el paquete MS Office, documentos de Word y tablas de Excel. Con ello se pretende que sólo el autor legítimo del documento pueda ver y modificar los datos confidenciales que contenga. Por desgracia, las funciones de contraseña de la mayoría de aplicaciones estándar no son en absoluto seguras. Los fabricantes de software no suelen preocuparse gran cosa de encriptar las palabras clave por medios complicados. Más bien las esconden con mayor o menor habilidad. Esto puede deberse a que se pretendan dejar abiertas posibilidades para que los usuarios olvidadizos puedan acceder a sus archivos protegidos. Actualmente, ya existen muchos programas especializados en desencriptar las contraseñas de determinadas aplicaciones, o en burlar la protección por contraseña. En estos casos, no suele importar lo astutamente que usted haya podido elegir su contraseña y lo segura que sea. Si quiere convencerse por sí mismo de lo poco fiable que es la protección por contraseña de sus aplicaciones favoritas, podrá hacerlo con la versión de prueba del programa *OfficePassword*, que podrá descargar en la siguiente dirección http://www.officepassword.com. El repertorio de este programa incluye, entre

otras funciones, todas las aplicaciones de Microsoft, pero también otros productos como el software financiero Quicken o el formato de compresión ZIP. En todos estos productos, el programa puede averiguar a partir de un documento existente la contraseña con la que va protegido. Los creadores prometen incluso una garantía de éxito al 100%, aunque sólo para los clientes de la versión completa ilimitada de OfficePassword. Pero la versión demo también sirve para que se convenza de lo sencillo que es desencriptar las contraseñas a las que se atribuye tanta seguridad.

Forzar archivos ZIP protegidos por contraseña

En el siguiente ejemplo, mostramos cómo se puede forzar con OfficePassword la contraseña de un archivo ZIP. Para eso, no se necesita más que el software y un poco de paciencia. Según la longitud de la contraseña, el proceso podrá tardar algunas horas o, si es extremadamente largo, incluso días. Pero si se dispone de información adicional, como puede ser la longitud probable de la contraseña o quizá, los signos que contiene, el proceso se podrá acortar considerablemente.

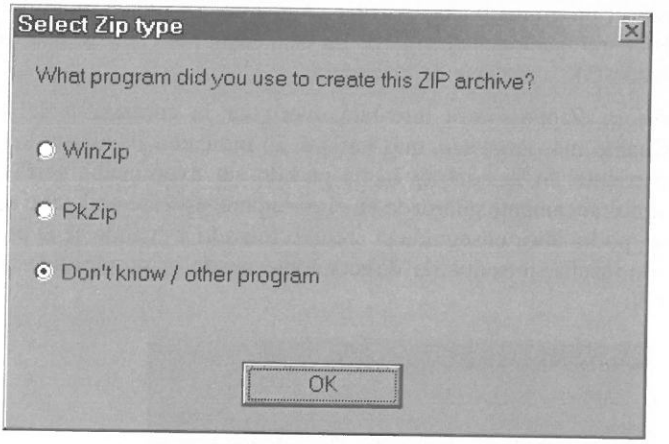
1. Arranque con *Inicio/Programas/OfficePassword/ZipPassword* el módulo especial para los archivos ZIP codificados.



OfficePassword dispone de un módulo especial para forzar archivos ZIP.

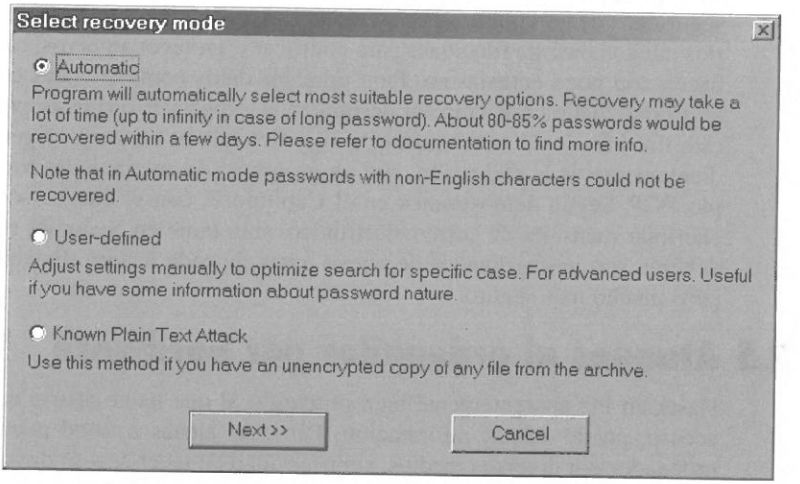
2. Aquí, haga clic sobre el botón *Select archive to crack* y en el diálogo de selección de archivos que aparecerá a continuación, introduzca el archivo ZIP que contenga el archivo codificado.

3. Después ZipPassword preguntará con qué programa ZIP se creó el archivo. Si se dispone de esa información, el proceso de descodificación podrá ser simplificado y acelerado. Pero tampoco importa si no se sabe. En este caso, seleccione simplemente la opción *Don't know / other program.*



Especifique (si lo sabe) con qué programa ZIP se generó el archivo.

4. Ahora, ZipPassword prepara la rutina de búsqueda. Después, usted podrá elegir cómo debe producirse el ataque a la contraseña. Por regla general basta con el modo *Automatic*, que no requiere mayores preparativos. Si la contraseña es muy larga, podrá acortar la búsqueda con otras opciones si dispone de información adicional sobre la contraseña.

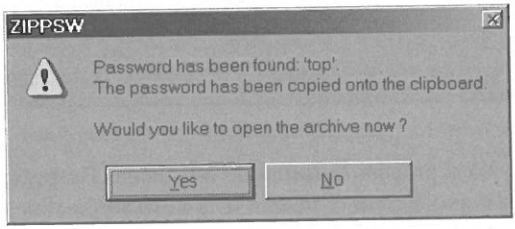


Elija el modo automático si no tiene información detallada sobre la contraseña.

5. En el siguiente paso puede indicar una lista de palabras *(dictionary file)*, con la que se deba perpetrar el ataque. Esta lista la podrá confeccionar usted mismo, o descargarla de Internet. Pero también se puede hacer sin lista, ya

que el programa puede ejecutar un ataque por fuerza bruta probando todas las combinaciones de signos. En este caso, sólo deberá hacer clic sobre el botón OK y armarse de paciencia.

6. Ahora, ZipPassword intentará averiguar la contraseña del archivo ZIP. Cuanto más larga sea, más tardará. El indicador de estado le mantendrá al corriente. Si la contraseña ha podido ser averiguada, será visualizada y simultáneamente guardada en el portapapeles. Haciendo clic sobre el botón *Si*, podrá abrir enseguida el archivo forzado y cuando se le pregunte por la contraseña, introducirla directamente desde el portapapeles con *[Ctrl] + [V]*.



ZipPassword ha desencriptado con éxito la contraseña de nuestro archivo de prueba.

Este ejemplo nos demuestra que no se puede ni se debe confiar en la "función de seguridad" de las aplicaciones estándar. Las aplicaciones que ofrecen a sus usuarios adicionalmente funciones para codificar o proteger archivos, casi siempre lo hacen con poco entusiasmo. Para proteger datos confidenciales con verdadera seguridad, habría que emplear herramientas especiales dirigidas expresamente a este fin. Para los documentos, esto significa que es mejor protegerlos independientemente de la aplicación, con un programa de encriptación como por ejemplo PGP. Según demostramos en el Capítulo 7, con el que no sólo se pueden encriptar mensajes de correo electrónico, sino también cualquier archivo. Éstos deberán ser desencriptados de nuevo antes de cada lectura. Es algo incómodo, pero mucho más seguro.

2.5 Ataques al ordenador por hardware

Hasta un PC aparentemente bien protegido al que nadie aparte de usted tenga acceso, puede delatar información. Personas ajenas a usted pueden espiar su ordenador por diversos medios, sin necesidad de tener acceso directo a él. Estos ataques no se basan en programas o puertas traseras. Trabajan a nivel puramente físico. Por eso, no pueden ser simplemente anulados por una hábil configuración o un software de protección especial. Deben ser combatidos con una técnica costosa. Por otro lado, para tranquilidad de la mayoría de usuarios de ordenador: estas técnicas de espionaje son tan costosas por sí mismas, que sólo sue-

len ser empleadas en el ámbito de los servicios secretos, la vigilancia estatal y el espionaje industrial. No es de suponer, que un usuario particular "medio" tenga razones para temer que el vecino de al lado haya pinchado sus sesiones de Internet. Aunque... nunca se puede saber con certeza.

INFO

Interceptar monitores de ordenador incluso desde cientos de metros de distancia

Los monitores de ordenador irradian un campo electromagnético tan fuerte, que incluso puede ser percibido desde cientos de metros de distancia. Poseyendo el equipo técnico necesario, se puede captar y amplificar esa radiación para reproducir la imagen original en otro monitor. Los servicios secretos ya llevan años aprovechando este fenómeno para fines de espionaje. Una furgoneta con algo de equipamiento técnico aparcada discretamente ante la casa, basta para espiar a la víctima con eficacia.

Señales ópticas y acústicas

Un método relativamente sencillo consiste en interceptar la información tanto óptica como acústica que se producen al trabajar con un ordenador. La información óptica más importante es la pantalla del mismo. Quizá usted tenga colocado el monitor de tal manera, que trabaje de espaldas a una ventana. En este caso, un espía armado con unos buenos prismáticos o un teleobjetivo, por poner un ejemplo, podría observar su pantalla a través de la ventana desde la finca vecina. Si, además, acoplara un aparato de reproducción visual a una videocámara y grabara todo, podría analizar después en cámara lenta hasta grabaciones rápidas y complejas. Aparte de la pantalla, podría espiar al propio usuario y así registrar la introducción de una contraseña.

Cuando se trabaja en un ordenador, el teclado también produce señales acústicas. Aunque al oído humano le resulten difíciles de diferenciar, cada tecla produce un ruido muy característico. Estas diferencias podrían ser registradas con aparatos de medición muy exactos, para así aislar las diferentes teclas. Como cada teclado suena de un modo diferente, los espías deberán poseer un perfil acústico del teclado que quieran espiar, para poder asignar a cada golpe una tecla. Existen dos posibilidades para hacerse con este perfil acústico:

- Al comienzo de su escucha, el espía se procura acceso al ordenador y averigua los sonidos típicos de cada tecla. Este proceso es rápido y eficaz, aunque trae consigo un gran riesgo.
- Algo menos peligroso resulta, si el fisgón tiene tiempo. Para cada tecla del teclado de un ordenador, hay una frecuencia estadística de utilización. Así, si escucha ese teclado durante un tiempo prolongado y se registra exactamente con qué frecuencia se produce cada ruido, después de un rato podrá asignar a cada ruido la tecla probable. Este método es menos eficaz, porque esa asignación nunca se puede hacer con una probabilidad del cien por cien.

Protección contra escuchas ilegales

La protección perfecta contra el espionaje óptico y acústico la ofrece un cuarto protegido visualmente e insonorizado, cosa que para la mayoría de usuarios seguramente no resultaría factible ni demasiado agradable. Pero también con nuestro comportamiento podemos ponérselo más difícil a los espías.

- Usted puede impedir con relativa rapidez la vigilancia óptica del monitor y el teclado. Procure que ni la pantalla ni el teclado puedan ser vistos desde una ventana. Lo mejor sería que el monitor del ordenador estuviera situado entre usted y la ventana. Así, se protegería sin medios adicionales de las miradas de curiosos.
- Protegerse de escuchas resulta algo más difícil. Una posibilidad está en procurar que siempre haya un ruido de fondo mientras esté trabajando en el PC. Para esto serviría una radio o un televisor. Si a usted le molesta el ruido constante durante el trabajo, hay una solución algo más tranquila. Acostúmbrese a toser con fuerza cada vez que introduzca datos delicados como podrían ser las contraseñas. Así tapará el sonido del teclado y no dará ninguna oportunidad a los espías.

Radiación electromagnética

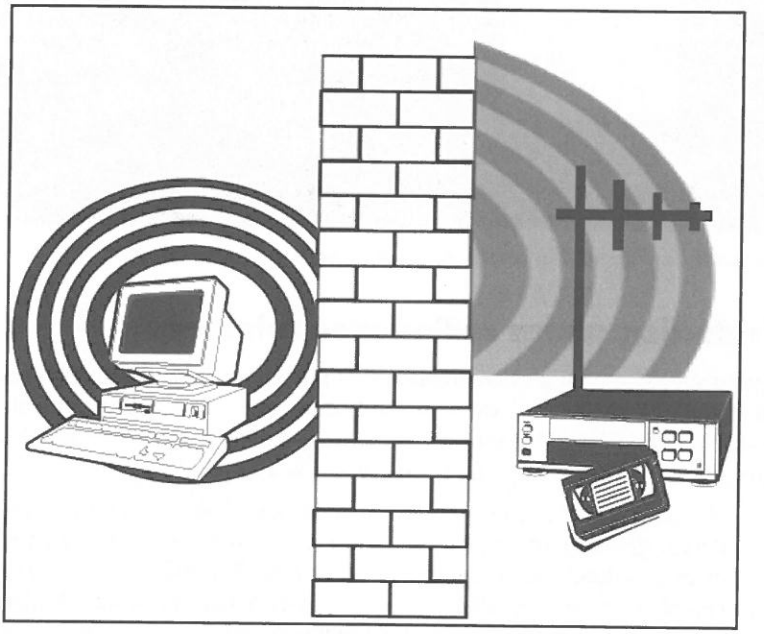
Todos los aparatos electrónicos generan una radiación electromagnética. Un ordenador está integrado por una amplia gama de estos componentes, por lo que produce una radiación electrónica correspondientemente elevada. Ésta crea lo que se denomina como smog electrónico, una contaminación ambiental que aún no ha sido investigada a fondo. Pero, lo más importante: utilizando aparatos que tengan la sensibilidad apropiada se puede analizar esta radiación para intervenir la información del ordenador.

INFO

TEMPEST

Una expresión empleada con frecuencia en cuestiones de radiación electromagnética es *TEMPEST*. Significa *Transient Electromagnetic Pulse Emanation Standard*, que podría traducirse como "Estándar para la radiación de impulsos electromagnéticos pasajeros". En los Estados Unidos, ya fue descubierto y analizado en los años cincuenta el peligro que emana de esta radiación. En aquel tiempo fue creado el Standard TEMPEST, que describe tanto el propio fenómeno como las contramedidas necesarias. Los aparatos a los que se atribuye homologación TEMPEST, no emanan impulsos electromagnéticos medibles, por lo que no pueden ser interceptados. Pero los PCs convencionales NO son aparatos con homologación TEMPEST, sino que reparten estas emisiones con toda la alegría del mundo. Podrán encontrar información detallada y links sobre el tema TEMPEST en la dirección: http://www.eskimo.com/~joelm/tempest.html.

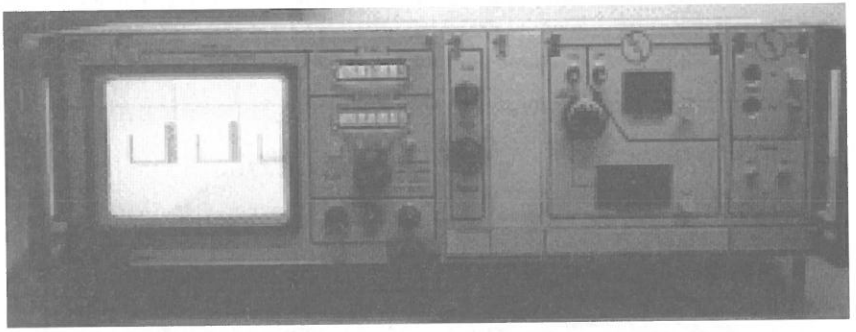
La fuente más intensa de radiación electromagnética es el monitor, por trabajar con voltajes de servicio muy altos. Pero también las tarjetas gráficas y los cableados que van entremedias son susceptibles de ser atacados. Estos componentes resultan tan apropiados como puntos de ataque, porque empleando recursos relativamente sencillos, permiten reproducir la imagen del monitor a través de una distancia de cientos de metros. El principio a aplicar para interceptar un monitor es relativamente sencillo. Todo lo que se necesita es una antena sencilla, osciladores para la sincronización de la pantalla y un aparato de reproducción visual. Para esto puede servir un televisor de los que hay en el mercado o, mejor aún, una grabadora de vídeo, que registrará todo y también permitirá analizar después a cámara lenta hasta acciones rápidas y complejas.



Así de sencillo es interceptar la radiación electromagnética.

¿Le suena todo esto a mitología de hackers? Hace algunos años, la Escuela Técnica Superior de Aquisgrán comprobó las posibilidades de esta técnica con un experimento. Utilizando un sencillo televisor y algún equipamiento adicional, los científicos lograron seguir, desde cierta distancia, lo que ocurría en una pantalla de PC. La distancia depende aquí de cuántas otras fuentes de radiación electromagnética haya en el entorno, y oscila desde algunos metros hasta un kilómetro. Tampoco sirve de mucho que funcionen al mismo tiempo varios aparatos, por ejemplo, en una sala de ordenadores especial. Hasta con 25 aparatos diferentes, se pueden aislar señales independientes.

Para los espías ahorrativos, los viejos televisores rusos en blanco y negro son un auténtico chollo. Esto se debe a que antiguamente la emisión televisiva era muy mala en la Unión Soviética, por lo que los televisores iban equipados con un receptor muy potente, capaz de visualizar hasta las señales más débiles. Pero quien quiera invertir más, podrá espiar con mayor eficacia aún. Utilizando un equipo más potente que costaría algunos millones de Ptas., no sólo se puede visualizar la imagen, sino también descodificar y registrar directamente las señales digitales.



Con aparatos especiales se puede espiar casi cualquier monitor de PC.

Protección contra radiaciones delatoras

Para protegerse contra el espionaje de la radiación electromagnética, existen – en función del bolsillo – varias posibilidades. Van enfocadas principalmente a evitar la radiación de los propios aparatos, o a taparla mediante impulsos parásitos con tal fuerza, que ya no pueda ser aislada la señal original.

- El método más seguro para evitar toda radiación, es colocar al ordenador dentro de una jaula de Faraday. Esta reja podría rodear, por ejemplo, todo el cuarto donde se encuentre el ordenador. Sin embargo, esto exige gran cantidad de obras y, además, no a todo el mundo le gusta trabajar en una habitación sin ventanas. También hay ordenadores cuya carcasa, inclusive el monitor, va rodeada por una jaula de Faraday. Pero estos modelos especiales son muy caros y sólo se venden a organismos gubernamentales.
- Si usted es un manitas, podrá construirle a su ordenador su propia jaula de protección. Encontrará la instrucciones correspondientes en Internet, por ejemplo bajo la dirección:

  http://www.austinlinks.com/Crypto/tempest.html.

- En el mercado de artículos para la seguridad existen algunos sprays que, según se dice, minimizan la radiación si son pulverizados sobre la cara interior de la carcasa del monitor y la del ordenador. Pero la eficacia de estas medidas es discutible.
- Mucho más eficaces son los emisores perturbadores, que tapan la radiación electromagnética mediante impulsos parásitos. Pero resultan muy caros y sólo protegen a los aparatos que se encuentren en su entorno inmediato. Además, el empleo de estos aparatos no suele estar permitido y puede traer consigo severas sanciones.

INFO

FTZ –¿protegido contra interferencias?

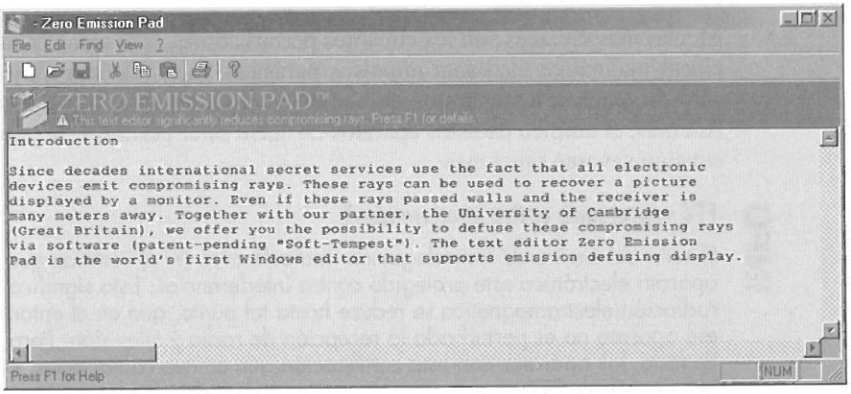
El sello del Centro de Homologación Radioeléctrica (FTZ) certifica que un aparato electrónico esté protegido contra interferencias. Esto significa que su radiación electromagnética se reduce hasta tal punto, que en el entorno de ese aparato no es perturbada la recepción de radio y televisión. Pero a pesar de todo, los aparatos con esta certificación aún emiten radiaciones, por lo que el símbolo FTZ no quiere decir que un ordenador esté protegido contra el espionaje.

Ahora bien, quien tema seriamente a los espías, podría pensar en comprarse un PC protegido contra TEMPEST. Pero esto no es factible así como así. Hay en todo el mundo un puñado de empresas que fabrican estos aparatos. Pero aparte de sus precios desorbitados, apenas existe la posibilidad de comprar legalmente un hardware protegido contra TEMPEST, ya que estas empresas especiales suministran exclusivamente a organismos gubernamentales, servicios secretos y ejército. Sin embargo, de vez en cuando podría surgir la oportunidad de adquirir a buen precio aparatos de segunda mano procedentes del ejército (http://www.eskimo.com/~joelm/tempestmisc.html).

Software contra TEMPEST

Aunque la interceptación de la emisión electromagnética suponga un ataque por hardware, hasta ciertos límites se le puede hacer frente con software. ¿Cómo se hace? Configurando el contenido de la pantalla de tal manera, que sea lo más difícil posible de espiar. Existe un programa para hacerlo, *Zero Emission Pad*, que puede ser descargado como freeware en la dirección http://www.demcom.com/en/zep/index.htm. Se trata de un editor de textos que trabaja con un juego de caracteres especial. Éste no sólo es comparativamente pequeño sino también muy borroso, por lo que resulta algo difícil de leer. Pero no sólo para usted sino para cualquier espía, que de por sí tendrá peor imagen en su monitor de espionaje. Las letras de trazo suave reducen considerablemente la radiación de estos puntos de imagen. Así, resultan difíciles de registrar. Pero la fiabilidad de esta protección depende siempre de la fuerza general que tenga la

radiación, de la distancia a la que se encuentre el fisgón y de la calidad del equipo. En resumen, no existe ninguna garantía de que realmente no haya alguien espiando.

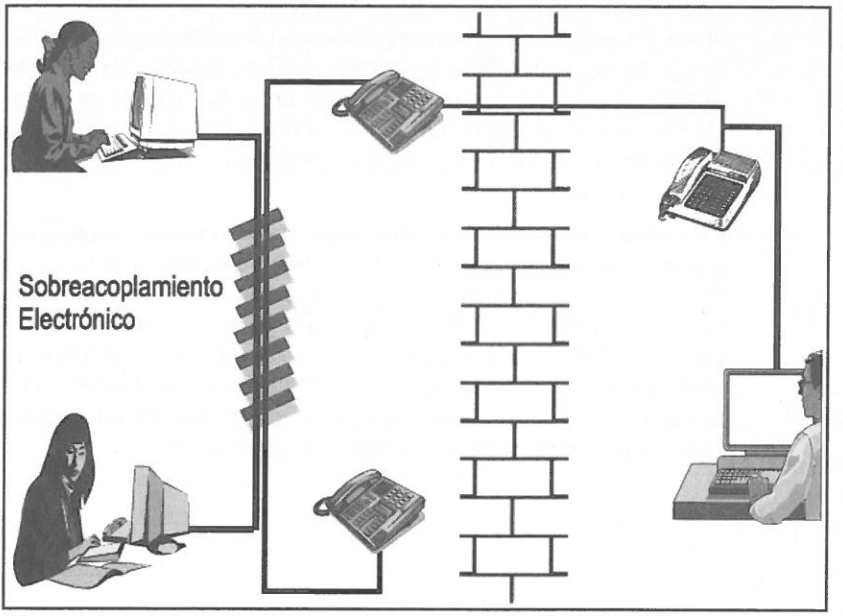


Con Zero Emission Pad, es posible protegerse de la radiación electromagnética.

Zero Emission Pad sirve para escribir y leer textos muy confidenciales, que de ningún modo deban llegar a manos de terceros. Pero para el trabajo de cada día resulta menos indicado, ya que la lectura de las letras resulta bastante fatigosa para la vista.

Interceptar el cable mediante sobreacoplamiento

Existe otro método de interceptación electrónica, basado en un sencillo fenómeno físico. Si se tienden en paralelo dos líneas eléctricas durante un determinado recorrido, se produce lo que se llama efecto de sobreacoplamiento. Al mandar a través de una de estas líneas datos en forma de diferentes tensiones eléctricas, las oscilaciones de tensión se trasladarán parcialmente a la línea de recorrido paralelo, sin necesidad de que exista contacto físico entre ambas. Por consiguiente, utilizando aparatos lo suficientemente sensibles, existe la posibilidad de registrar en una de las líneas la información que sea transmitida a través de la otra.



El principio de la interceptación mediante sobreacoplamiento electrónico.

Sobre todo para los ordenadores integrados en una red, el sobreacoplamiento supone un grave peligro. En los edificios de oficinas, las conexiones de la red suelen ir tendidas en canalizaciones de suministro, donde se juntan con los cables de la luz, el teléfono y la calefacción. En teoría, esto permitiría establecer con una simple llamada telefónica un vínculo con la red de distribución del edificio, para interceptar desde allí el tránsito de datos. En la práctica no resulta tan sencillo. Pero generalmente, basta con pinchar una línea en cualquier punto del edificio. Aunque en este caso, costaría más analizar la información. En primer lugar, habría que aislar y amplificar las señales muy débiles mediante aparatos de medición sensibles. La información así obtenida tendría que ser analizada y reproducida. Esto es un proceso muy costoso que requiere conocimientos específicos. Por lo tanto, no hay motivos para temer que su vecino le esté espiando de esta manera, salvo que sea ingeniero eléctrico y especialista en ordenadores.

Protección contra los efectos de sobreacoplamiento

Es posible protegerse contra el sobreacoplamiento por varios medios. Todos son bastante costosos, aunque también la intercepción por sobreacoplamiento es un asunto complicado y caro. Por esta razón, se emplea sólo en el ámbito del servicio secreto y el espionaje económico, por lo que generalmente sólo necesitan protección estos sectores.

- La protección más eficaz contra el sobreacoplamiento consiste en evitarlo desde el principio. Esto se puede conseguir limitadamente con aislamientos de cables especiales. Pero lo mejor es tender los cables de la red totalmente separados de las demás líneas. Este principio aún puede ser tenido en cuenta cuando se diseña un nuevo edificio. Pero en las instalaciones ya existentes una reforma a posteriori resulta casi imposible y en cualquier caso, muy costosa.
- Para esos casos queda el método algo más económico, también algo más inseguro, de enviar todos los datos siempre encriptados a través de la red. Existe la posible de hacer que la encriptación la realicen protocolos de red especiales. Las tarjetas de red especiales poseen su propio chip de codificación y cifran los datos por hardware. De este modo se alcanza un gran nivel de seguridad, sin menoscabo de la velocidad de los datos. Por norma, la encriptación del flujo de datos en la red siempre es tan segura como lo sean los procedimientos de encriptación empleados.

3 Nivel de seguridad 2: peligros procedentes de Internet

3.1 El navegador web: una fuente de riesgo. Qué puede suceder 124
Los peligros del PC conectado 124
Peligros online en el ámbito privado 126
Peligros online para su bolsillo 126

3.2 Conceptos de seguridad – las funciones protectoras de los navegadores 127
Zonas y niveles de seguridad en Internet Explorer 127
Las opciones avanzadas de seguridad de Internet Explorer 135
Las funciones de seguridad de Netscape Navigator 139
Peligros causados por agujeros de seguridad 146

3.3 Un PC teledirigido – los peligros del ActiveX, JavaScript & Co. 151
Utilidad y riesgos de los contenidos activos en páginas web 152
Desactivación fiable de los componentes ActiveX 153
Impedir la ejecución de Java-Applets 156
Peligros causados por scripts dinámicos 160
Medidas de prevención con los Plug-Ins 166

3.4 Virus y troyanos – protección contra infecciones digitales 168
Protección eficaz contra los virus 169
Escáner antivirus – ¿Doy positivo? 173
Espías en la sombra – los caballos de Troya 185
Cuarentena – verificar cuidadosamente el software nuevo 191

Internet, debido al amplio número de posibilidades que ofrece, hechiza a todo tipo de personas. Entre éstas, no sólo nos encontramos a internautas formales y honestos; también están las inevitables ovejas negras. Y no es de extrañar. Al fin y al cabo, Internet permite moverse con cierto anonimato y, aplicando medios sencillos, se puede atacar a una gran cantidad de víctimas. Son especialmente perniciosos los malhechores que no buscan ganancias materiales, sino únicamente divertirse causando daño a los demás. Desarrollan virus, páginas web de

peligrosos contenidos activos y caballos de Troya que les servirán para espiar o incluso estropear los PCs de otros usuarios. El móvil de estas personas es simplemente la curiosidad técnica o el afán de notoriedad. Quieren ser reconocidos como verdaderos hackers en los círculos de mayor relevancia, y no tienen escrúpulos a la hora de conseguir sus "logros" a costa de otros. En este capítulo, queremos mostrarles los peligros que acechan al navegar por Internet y cómo se les puede hacer frente con eficacia.

3.1 El navegador web: una fuente de riesgo. Qué puede suceder

Hoy en día, cada vez que iniciamos una sesión de Internet con el PC, nos exponemos, por desgracia, a un riesgo potencial. Los peligros más variopintos le acechan para golpearle sin piedad. En la prensa del ramo, aparecen constantemente noticias de este tipo bajo llamativos titulares. El tema es explotado regularmente en algunos programas de televisión, que recurren a él para atraer a los espectadores. En las próximas páginas, pretendemos mostrar sin afán de sensacionalismo qué hay de cierto en todo ello. Para empezar, vamos a establecer una distinción entre tres clases de peligros:

- *Peligros para el PC*, es decir, riesgos que puedan causar el deterioro o la pérdida de datos.
- *Peligros para el entorno privado*, por los que datos personales y confidenciales puedan llegar a manos de personas no autorizadas.
- *Riesgos para el bolsillo*, que le hagan perder mucho dinero. También los dos primeros tipos pueden acabar originando costes elevados.

Los peligros del PC conectado

Como el PC es la herramienta con la cual se conecta a Internet, es natural que sea el primero en exponerse a los riesgos. Aquí, el peligro planea ante todo sobre lo más valioso que contiene el PC, es decir, los datos que ocupan el disco duro en forma de archivos y directorios. Desgraciadamente, estos datos se encuentran fuertemente amenazados.

Virus informáticos

Ciertamente, los virus informáticos forman el elemento de riesgo más frecuente y más antiguo para los ordenadores. Ya se les conocía y temía en tiempos del ordenador doméstico. Desde entonces, han mejorado considerablemente tanto en calidad como en cantidad. Sobre todo, Internet ha conferido al problema de los virus informáticos una dimensión totalmente nueva. Mientras que antiguamente

un virus necesitaba semanas o meses para propagarse mediante un disquete, hoy en día puede viajar por todo el globo terráqueo en cuestión de pocas horas. Por ello, cada vez que se descarguen archivos resulta imprescindible asegurarse de no haber contraído uno de esos parásitos digitales.

Una variedad especialmente peligrosa de virus son los troyanos o caballos de Troya, que simulan ser una aplicación útil, aunque en realidad lo que hacen es espiar clandestinamente al usuario o destruir sus datos.

INFO

¿Es posible que los virus o caballos de Troya causen también daños de hardware?

Desde el punto de vista puramente teórico, un virus o caballo de Troya también podría causar daños al hardware. Resultaría imaginable, por ejemplo, un programa que eleve muy por encima del valor límite permitido la frecuencia de actualización o refresco del monitor. En los monitores antiguos, esto podría causar un daño definitivo. No obstante, las pantallas modernas poseen los correspondientes circuitos de protección para evitar este tipo de averías. Otros dispositivos hardware sólo podrían ser dañados con gran esfuerzo y muy buenos conocimientos sobre los componentes en cuestión. Aunque constantemente surgen rumores acerca de que los sectores de arranque o las tablas de asignación de archivos de los discos duros pueden ser inutilizados para siempre mediante software. Pero hasta ahora, nadie ha aportado una prueba concluyente. En resumen, el riesgo de que el hardware sufra daños a causa de un virus u otro tipo de programas destructivos, es francamente bajo. Por otro lado, un daño no tiene por qué ser de hardware para ser muy grave. El reformateo de un disco duro donde quizá se almacenara el trabajo de varios meses o incluso años, es verdaderamente grave.

Contenidos activos

Un peligro típico de Internet son los contenidos activos. Éstos se basan en páginas web que no sólo representan textos e imágenes inmóviles, sino que también ofrecen contenidos dinámicos o brindan al usuario la posibilidad de interacción. Un ejemplo de estos componentes activos podría ser un juego de Tetris unido a una página web (lo que no significa que el Tetris suponga un peligro – en todo caso para la salud mental). La cosa adquiriría otro cariz, si por ejemplo el programador de este juego de Tetris no estuviera sobrado de talento y hubiera hecho un trabajo chapucero, por lo que podría causar caídas del sistema y/o pérdidas de datos en su PC (a fin de cuentas, quien ejecuta estos componentes activos).

Si el programador fuera hábil y malévolo, también podría configurar sus componentes activos de tal manera, que dañen o espíen selectivamente determinados datos. De esta forma, los hackers exhibicionistas del "Chaos-Computer-Club" mostraron hace algún tiempo un componente ActiveX, con el que ordenaron a un software de banca electrónica instalado en el ordenador de un usuario, que transfiriera dinero desde la cuenta de éste a la del CCC. Podrán encontrar una

descripción más detallada de este suceso en la dirección http://www.ccc.de/radioactivex.html.

Peligros online en el ámbito privado

Todo aquel que navega por Internet, se pone muchas veces en peligro al exponer más datos personales y confidenciales de lo que quizá quisiera. Aquí habría que distinguir entre los datos que se comunican voluntariamente y los que alguien sonsaca mediante trucos.

Protección contra el correo indiscriminado

Los datos pueden y deben ser comunicados muchas veces en Internet. Por ejemplo, a la hora de hacer pedidos en una tienda virtual, es imprescindible indicar la dirección y la cuenta bancaria, o la tarjeta de crédito. Pero también en concursos o juegos donde se dan premios y ofertas gratuitas, casi siempre quieren saber muchas cosas sobre el usuario. Frecuentemente, la oferta va financiada con publicidad, y los operarios venden esos datos a agencias publicitarias, que después bombardearán al usuario con propaganda dirigida selectivamente. Esto es más molesto que peligroso, aunque también hay peligros reales en el ámbito privado.

El internauta de cristal

A través de Internet, otros pueden saber mucho acerca de usted. Por el mero hecho de navegar, usted ya va dejando gran cantidad de huellas en su PC, en los ordenadores de su proveedor de redes y en los servidores de cuyas páginas hiciera uso. Si, además, toma parte activa en Internet, por ejemplo con sus propias páginas web o participando regularmente en grupos de noticias, los detectives online podrán confeccionarle un perfil de usuario en toda regla. Esto podría ser aprovechado por un hacker para obtener más información sobre usted y hacerse con sus contraseñas. Pero del mismo modo, un compañero de trabajo envidioso podría investigar en Internet y desenterrar algún cadáver (esperemos que virtual). En el Capítulo 8 le mostraremos de modo completamente práctico, como mantener el anonimato y el ámbito privado incluso en la vida online.

Peligros online para su bolsillo

De la actividad online también emanan riesgos para su bolsillo o su cuenta corriente. Cuando llega el momento de pagar a través de Internet, comienza el peligro, ya que es necesario indicar la cuenta bancaria o la tarjeta de crédito, y es que hasta ahora, no se han podido imponer formas de pago alternativas más

seguras. Por desgracia, estos datos en manos equivocadas valen su peso en oro. Alguna que otra ganga superbarata en Internet ya se ha revelado como un camelo, cuya única finalidad era obtener los datos de la tarjeta de crédito del comprador. Datos que luego sirven para que estos villanos hagan sus propias compras. Cuando usted pueda darse cuenta de los daños, ellos ya habrán puesto pies en polvorosa y quizá a usted le hayan birlado unos cuantos billetes.

Otra fuente de posibles riesgos financieros son las cada vez más populares banca y bolsa electrónicas, es decir, la tramitación de negocios bancarios y de bolsa a través de Internet. También aquí, hay en juego datos muy delicados. Si las claves de entrada y las firmas electrónicas caen en malas manos, se arma enseguida una de todos los diablos, y como los bancos con sus relaciones comerciales se quitan de encima cómodamente la responsabilidad, se quedará con el desaguisado. Resumiendo, también a la hora de tramitar negocios bancarios por Internet conviene aplicar unas medidas de prevención muy especiales.

3.2 Conceptos de seguridad – las funciones protectoras de los navegadores

Como los navegadores web son las herramientas para navegar por Internet, naturalmente también ofrecen la superficie de ataque mayor. Al mismo tiempo, sirven como baluarte contra ataques y contenidos destructivos en la Red. Eso lo tienen en cuenta los desarrolladores de los navegadores actuales, equipando sus productos con extensas funciones de seguridad de mayor o menor eficacia. Para poder navegar con seguridad, es importante que se comprendan y aprovechen esos conceptos de seguridad. Así, existe la posibilidad de automatizar muchas reglas de seguridad y medidas preventivas de gran importancia, que permitan navegar sin preocupaciones.

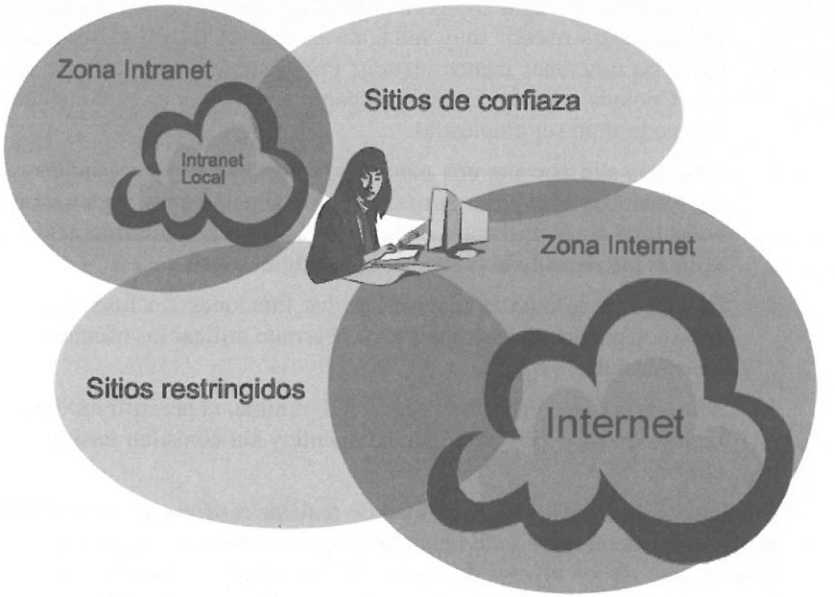
Zonas y niveles de seguridad en Internet Explorer

El concepto de seguridad de Internet Explorer de Microsoft se subdivide en dos partes. En primer lugar, este navegador ofrece un sistema flexible de *Zonas de seguridad*, que permite adaptar prácticamente a cualquier sitio web las configuraciones de seguridad más importantes. Aparte de esto hay una serie de *Niveles de seguridad*, cada uno de los cuales proporciona un determinado grado de seguridad, sin que los usuarios menos expertos tengan necesidad de ocuparse detalladamente de las diferentes opciones y selecciones. Quien no acabe de fiarse de estas divisiones generales y prefiera ocuparse por su cuenta de las configuraciones, podrá hacerlo, ya que también se permiten niveles definidos por el usuario con configuraciones totalmente personalizadas.

Zonas de seguridad

Internet Explorer permite clasificar cada página web por su dirección en una de las cuatro zonas de seguridad posibles. Para cada una de esas cuatro zonas de seguridad, se puede crear el número de opciones de seguridad que se desee. Por ejemplo, según si para sitios web de una determinada zona hay que ejecutar o no controles ActiveX o scripts en las páginas web. Cuando carga una página web, Internet Explorer comprueba a qué zona de seguridad pertenece. Las páginas que no fueran asignadas propiamente, son adjudicadas automáticamente a la zona general de Internet. Esta asignación se realiza según la dirección de la página web. En función de ésta, se restringirán las posibilidades de acceso al documento y sus contenidos según las especificaciones del usuario.

- En la zona de *Intranet Local* se incluyen todos los documentos web procedentes del propio ordenador o de un servidor web de la misma subred, por ejemplo una intranet de empresa. Se puede suponer que de estos documentos emana poco peligro, ya que no cabe esperar amenazas intencionadas desde el entorno más cercano. La inclusión de las páginas web dentro de esta zona se hace automáticamente en función de la dirección.
- La zona *Sitios de confianza* contiene las direcciones web que a usted le parezcan inofensivas. Para que Internet Explorer cambie a la zona de confianza cada vez que solicite estos documentos, deberá asignar una vez la dirección a esa zona (más adelante profundizaremos en este tema). Es importante que sólo asigne a esta zona páginas u ofertas fiables, ya que aquí rigen por norma reglas de seguridad relativamente generosas.
- La zona *Sitios restringidos* es un área de cuarentena pensada para las páginas web peligrosas. Por norma tiene unas configuraciones de seguridad muy restrictivas, de modo que los contenidos destructivos no tengan la menor oportunidad. Si usted cree que una página web contiene un peligro concreto, debería incluir su dirección en esta zona antes de visitarla por primera vez.
- Finalmente, la zona *Internet* incluye el resto de las páginas que no fueran asignadas a ninguna de las tres primeras zonas, ya fuera automáticamente o en función de la clasificación manual hecha por usted mismo. Si Internet Explorer activa una página que no esté asignada a ninguna de las otras zonas, cambiará automáticamente a ésta, donde, por lo tanto, deberían regir unas reglas de seguridad relativamente estrictas.



Las zonas de seguridad de Internet Explorer.

TRUCO

Identificar la zona de seguridad activa en ese momento

Mientras navega con Internet Explorer, tiene la posibilidad de comprobar en todo momento, en qué zona de seguridad se encuentra. El navegador informa de la zona elegida en ese momento a través de la línea de estado situada en el margen inferior derecho de la ventana.

En la línea de estado aparece la zona de seguridad que esté activa en ese momento.

Niveles de seguridad

Por norma, Internet Explorer asigna a cada zona un nivel de seguridad previamente definido. Cada uno de estos niveles contiene configuraciones de seguridad con diferentes restricciones. Por cada zona de seguridad se pueden ajustar multitud de configuraciones. Para no abrumar al usuario, Internet Explorer conoce diversas variantes de configuración predefinidas que pueden ser seleccionadas en función de las necesidades de seguridad. Según el nivel de seguridad elegido, se emprenderán las configuraciones en sí. En total, hay cuatro niveles posibles.

- *Alto* permite navegar con gran seguridad, aunque en determinadas circunstancias podrá quedar muy reducida la funcionalidad, al ser desactivadas todas las funciones menos seguras. Por ejemplo, suele rechazar de plano a los "Cookies", con lo que algunas páginas web (por ejemplo tiendas virtuales) no podrán ser empleadas.
- *Mediano* aún permite una navegación bastante segura, estando casi todas las funciones activadas. Pero en las funciones menos seguras, primero se consultará al usuario antes de permitirlas. Con esta configuración se puede utilizar plenamente la mayoría de las páginas web.
- En *Bajo* se ejecuta la mayoría de las funciones (incluso algunas de las menos seguras) sin consulta previa. Permite utilizar las ofertas web en toda su extensión.
- *Muy bajo* trae consigo una seguridad mínima, al permitir todo tipo de contenidos activos. Ejecuta inmediatamente y sin consultar casi todas las funciones.

Finalmente, aún existe la posibilidad de realizar *configuraciones definidas por el usuario*, cambiando individualmente determinadas configuraciones sobre la base de uno de los niveles de seguridad. La siguiente tabla nos da una idea de los niveles de seguridad y la asignación estándar a las zonas de seguridad.

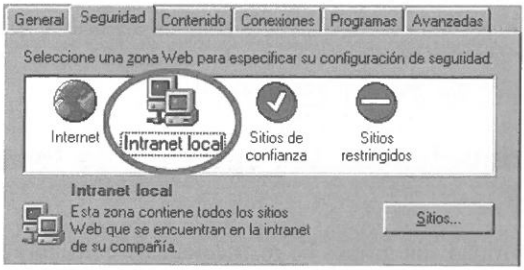
Zona	Nivel	Consecuencia
Intranet local	Mediano	Se advierte al usuario antes de activar contenidos que puedan ser dañinos
Sitios de confianza	Muy bajo	Prácticamente no hay limitaciones. Todos los contenidos son activados sin advertencia previa.
Sitios restringidos	Alto	El navegador web impide la activación de contenidos que puedan ser dañinos.
Internet	Mediano	Se advierte al usuario antes de activar contenidos que puedan resultar dañinos.

Asignación de zonas y niveles de seguridad

Los niveles de seguridad estándar ofrecen configuraciones útiles para las distintas zonas. Pero si usted lo necesita, también podrá modificar las asignaciones sin problema. Por ejemplo, podría darse el caso de que necesite seleccionar para la intranet local el nivel de seguridad *Bajo* por ser distribuidos en su red local controles ActiveX o Java-Applets con los que necesite trabajar.

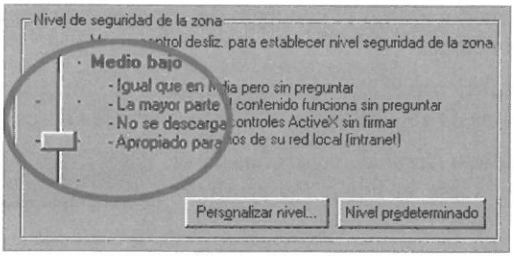
1. Si quiere elegir otro nivel de seguridad para una zona, abra con *Herramientas/Opciones de Internet...* las configuraciones de Internet Explorer y cambie a la categoría *Seguridad*.

2. En primer lugar, elija en la parte superior la zona de seguridad a la que desee asignar otro nivel de seguridad.



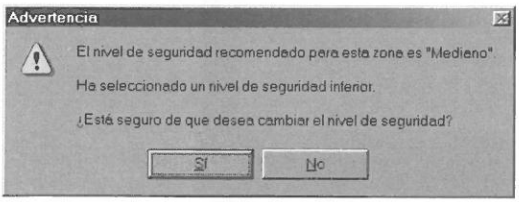
Elija en primer lugar la zona de seguridad deseada.

3. Bajo el apartado *Nivel de seguridad de la zona*, Internet Explorer muestra los niveles que tiene asignados a esa zona de seguridad en ese momento. Seleccione aquí el nuevo nivel.



Defina el nivel de seguridad para la zona de seguridad seleccionada en la parte superior.

4. Con algunas combinaciones de zonas y niveles de seguridad, Internet Explorer tiene sus reservas. IE se las comunicará mediante un mensaje de advertencia. Si quiere ignorar ese aviso y activar las configuraciones a pesar de todo, haga clic sobre el botón *Sí*. Si prefiere no correr riesgos y confiar en la recomendación de Internet Explorer, anule los cambios con el botón *No*.



Internet Explorer le advierte a usted si considera que las configuraciones son arriesgadas.

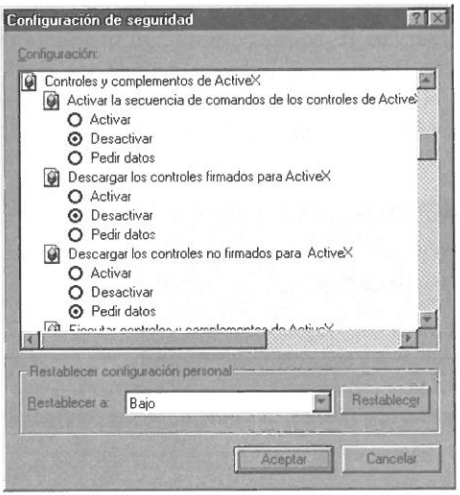
5. Para regresar a las configuraciones estándar originales, sólo tiene que hacer clic sobre el botón *Nivel predeterminado*. Tenga en cuenta que esto sólo restaura el nivel para la zona de seguridad seleccionada en la parte superior. Las configuraciones de las demás zonas permanecerán invariables o deberán ser restituidas una a una.

Ajustar individualmente las opciones de los niveles de seguridad

Los niveles de seguridad son grupos de restricciones y configuraciones previamente definidas, que ponen a disposición del usuario un concepto de seguridad a varios niveles. Pero no tienen por qué ser los más apropiados para cada situación. En especial, el hecho de que reciban el mismo tratamiento los peligrosos controles ActiveX y los Java-Applets, bastante más seguros, no siempre queda justificado. En estos casos, usted puede aplicar configuraciones propias personalizadas y, de este modo, ajustar el concepto de seguridad de Internet Explorer a sus necesidades concretas.

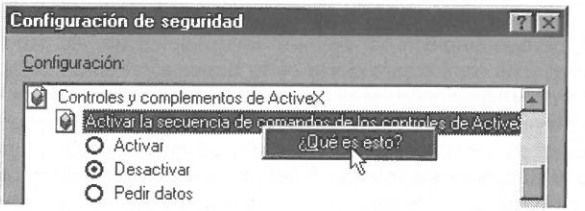
1. Active en *Herramientas/Opciones de Internet...* la categoría *Seguridad* y seleccione la zona de seguridad cuyas configuraciones desee modificar.
2. Dentro del apartado *Nivel de seguridad de la zona*, haga clic sobre el botón *Personalizar nivel...*

3. Aquí encontrará una extensa lista de configuraciones de seguridad. Para cada opción, podrá elegir entre varias posibilidades.



Las configuraciones de cada nivel de seguridad pueden ser ajustadas a un nivel absolutamente personal.

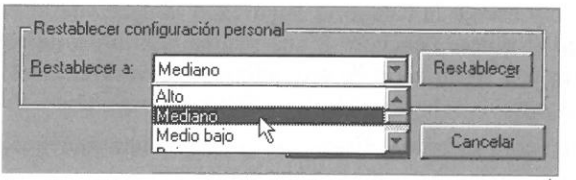
4. Si hace clic con la tecla derecha del mouse sobre una de estas opciones, abrirá el menú contextual con la función de ayuda directa. Ésta les brindará una breve explicación de cada entrada y sus posibilidades de configuración.



Con la ayuda directa, podrá mostrar una breve explicación para cada configuración.

5. Para la mayoría de entradas puede autorizar la respectiva función *(Activar)*, permitirla sólo tras consultar al usuario *(Pedir datos)* o hacer que el navegador la bloquee automáticamente *(Desactivar)*.

6. Si ahora quiere regresar a las configuraciones estándar, escoja en la lista de selección *Restablecer a:* el nivel de seguridad deseado *(Alto, Mediano, Medio bajo o Bajo)* y active con el botón *Restablecer* las correspondientes configuraciones estándar.



Con Restablecer, puede pasar de las opciones personalizadas a la configuración estándar.

7. Muy importante: para aplicar los cambios, concluya haciendo dos clics seguidos sobre el botón *Aceptar* de las respectivas ventanas de configuración.

Clasificar las páginas web en zonas de seguridad

Internet Explorer reconoce los sitios web procedentes de la intranet local o de Internet por su dirección. Pero las zonas de seguridad *Sitios de confianza* y *Sitios restringidos* sólo tienen sentido si incluye determinadas direcciones en estas zonas. Por lo tanto, si usted solicita una de las direcciones almacenadas, Internet Explorer cambiará automáticamente a la zona correspondiente y con ello, a las configuraciones de seguridad que le correspondan.

INFO

¿Qué direcciones hay que incluir en los sitios de confianza?

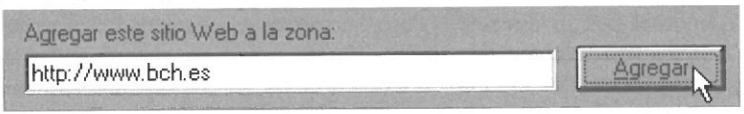
Como el propio nombre indica, usted sólo debería asignar a esta zona aquellos sitios web de los que tenga constancia que no son peligrosos. Pero esto no implica que enseguida deba asignar a esta zona todas las direcciones que le parezcan inofensivas. Dicha zona está pensada, sobre todo, para los sitios que no funcionen con las configuraciones de seguridad de la zona Internet, porque empleen por ejemplo Java-Applets que en esa zona no estén permitidos. Este caso puede darse en la banca electrónica, si su banco emplea Java-Applets para el acceso a la cuenta. Si usted desactivara en la zona de seguridad *Internet*, a la que por regla general pertenecería el servidor web de su banca online, la ejecución de Java-Applets, ya no podría acceder a su cuenta electrónica. Para resolver este problema, puede asignar la dirección del servidor web de su banco a la zona *Sitios dignos de confianza* y permitir en esa zona la ejecución de Java-Applets. De esta forma, ya no tendrá problemas cuando tramite online sus asuntos bancarios. Otros candidatos a ocupar su zona de confianza son las tiendas virtuales o páginas similares, que también requieren del uso de Java-Applets. Aunque es recomendable plantearse muy a fondo, cada vez que se quiera incluir una página web, si ésta es realmente "digna de confianza".

Para clasificar un sitio web dentro de las zonas *Sitios de confianza* o *Sitios restringidos*, tan sólo debe saber la dirección de esa página web. Y para eso, ni siquiera necesita conectarse y activar esa página.

1. Active las configuraciones de seguridad con *Herramientas/Opciones de Internet...* y escoja la categoría *Seguridad*. Seleccione la zona *Sitios de confianza* si quiere conceder a una página web unos derechos especialmente amplios. Si en lugar de eso quiere poner restricciones adicionales a un sitio peligroso, seleccione la zona *Sitios restringidos*.

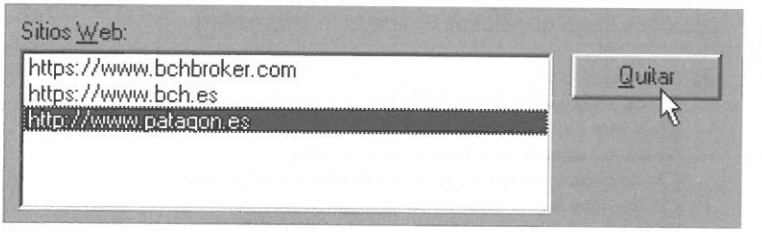
2. Haga clic sobre el botón *Sitios...* para incluir una nueva dirección en la zona seleccionada.

3. Para agregar una nueva dirección, introdúzcala en el menú que se muestra a continuación, concretamente en el campo de entrada *Agregar este sitio Web a la zona:*. Deberá indicar la dirección URL completa *(http://)*. Con el botón *Agregar* incluirá la dirección introducida en la lista.



Introduzca la dirección web de la página que pretenda incluir en esa zona.

4. Si lo que desea es eliminar una dirección introducida anteriormente, marque la entrada en la lista y bórrela con el botón *Quitar*.



Con Quitar puede volver a extraer de la zona determinadas páginas.

5. Con *Aceptar* incluirá la dirección nueva en esa zona. A partir de ahora, cada vez que active ese sitio web, Internet Explorer activará automáticamente esta zona con su correspondiente nivel de seguridad.

TRUCO

Verificación del servidor por https://

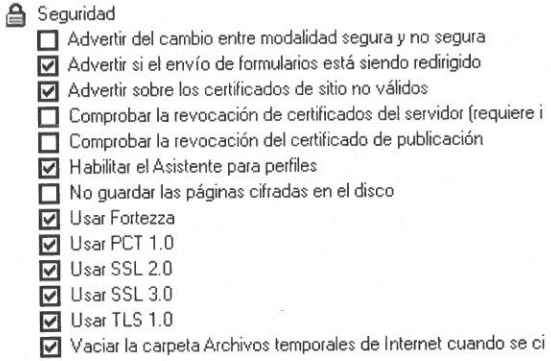
En el menú de sitios web dignos de confianza, encontrará, además, la opción *Necesita comprobación del servidor (https:) para todos los sitios de esta zona*. Esto significa que para acceder a las páginas web de la zona *Sitios de confianza*, sólo se deberán emplear conexiones seguras. Así, antes de establecer conexión con un sitio web, Internet Explorer verificará siempre si el servidor de ese sitio es seguro. Aunque, por regla general, esto no es necesario y tampoco lo soportan todos los servidores web, de modo que lo mejor es dejar desactivada esta opción.

La verificación del servidor garantiza la seguridad de una conexión.

Las opciones avanzadas de seguridad de Internet Explorer

Las configuraciones de los niveles de seguridad dependen de las zonas de seguridad. Es decir, se permiten configuraciones individuales basadas en la confianza o recelo que inspire determinada página web. Aparte de esto, Internet Explorer reconoce toda una serie de configuraciones de seguridad universales que no dependen de zonas de seguridad, sino que son válidas siempre para todas las páginas web. Se trata de configuraciones con las que se puedan activar y desactivar determinadas técnicas que proporcionan una seguridad especial (protocolos especiales para una transmisión de datos segura), o también ciertas funciones que suponen riesgos potenciales y por ello, pueden ser desactivadas por usuarios cautelosos.

Encontrará las configuraciones de seguridad avanzadas en las opciones de Internet (*Herramientas/Opciones de Internet...*) dentro de la pestaña *Avanzadas*. Utilice aquí la barra de desplazamiento para bajar por las diferentes opciones hasta que llegue al apartado *Seguridad*.



Las opciones avanzadas de seguridad de Internet Explorer.

Generalmente, para todas estas opciones, la activación de cada configuración incrementa la seguridad. Pero algunas opciones van unidas a restricciones funcionales o a que se necesite más tiempo durante la navegación. Las configuraciones estándar suponen un equilibrio bastante bueno entre seguridad y rendimiento. Con *Restaurar valores predeterminados*, podrá restablecer dichas configuraciones en cualquier momento.

Comprobar la revocación de certificados

Si Internet Explorer se encuentra con componentes cuyo origen vaya acreditado con un certificado, podrá comprobar si ese certificado sigue vigente. Para ello, deberá establecer contacto con el servidor del emisor del certificado y consultarlo. Esto requiere tiempo adicional, por lo que el propio usuario deberá decidir si le conviene para conseguir más seguridad.

- *Comprobar la revocación de certificados del servidor* dirige la verificación de los certificados de seguridad de páginas web.
- *Comprobar la revocación del certificado de publicación* avanza un paso más en la seguridad y verifica si el emisor de un certificado dispone a su vez de un certificado válido. De lo contrario, el propio proveedor podría extenderse a sí mismo un certificado como emisor.
- *Advertir sobre los certificados de sitio no válidos* indica si quiere que Internet Explorer le avise cuando la dirección que figura en un certificado no sea válida.

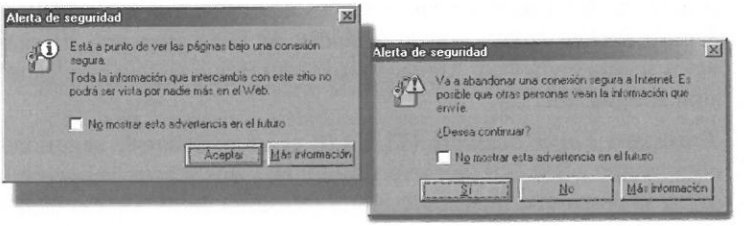
Recomendación:

- Si le da mucha importancia a la seguridad y, por ejemplo, tramita regularmente operaciones bancarias online o realiza compras a menudo, debería activar todas las opciones.
- Si le importa menos la seguridad y lo que desea es navegar lo más deprisa posible y evitar esperas innecesarias, desactive las dos primeras opciones. Pero, por si acaso, debería conservar al menos la tercera para que le advierta si el certificado no es válido.

Cambio entre conexiones seguras y conexiones inseguras

Para que usted sepa en todo momento si está utilizando una conexión segura o una insegura, cada vez que cambie de un enlace a otro, Internet Explorer le podrá advertir mediante una ventana de aviso. Para ello, deberá asegurarse de que esté activada la opción *Advertir del cambio entre modalidad segura* y no segura. A partir de entonces, Internet Explorer visualizará una ventana de aviso cada vez que cambie la modalidad de la conexión.

Recomendación: actívela



Así le avisa Internet Explorar cada vez que cambia de una conexión segura a una insegura y viceversea.

Borrar automáticamente la caché de Internet

Internet Explorer almacena en una memoria caché todos los documentos web solicitados, para que puedan ser cargados más deprisa cuando se les active de nuevo. Pero esto tiene una desventaja, y es que por las páginas web almacenadas en la memoria caché, los demás usuarios de su PC podrían enterarse de todo aquello por lo que usted se interesó durante su última sesión de Internet.

- Si quiere evitar esta situación, sería conveniente activar la opción *Vaciar la carpeta archivos temporales de Internet cuando se cierre el explorador.* En este caso, los datos temporales almacenados durante la sesión de Internet serán eliminados al finalizar Internet Explorer.

- Active, además, la opción *No guardar las páginas cifradas en el disco.* Con esto, las páginas web de contenido confidencial ni siquiera serán almacenadas en la memoria intermedia del disco duro. De lo contrario, a partir de la caché todos los usuarios podrían solicitar los datos confidenciales.

Recomendación: esta configuración depende de la importancia que se dé a la confidencialidad de los datos, o si otros usuarios tienen acceso al PC.

El empleo de los protocolos de seguridad

Las conexiones HTTP habituales de la Red se ejecutan desprotegidas en texto claro. Es decir, cualquiera puede averiguar con algo de esfuerzo técnico los datos que transmitimos. Cuando se navega por la red sin más, esto aún se puede consentir. Pero a la hora de realizar compras online, operaciones por banca electrónica u otras transacciones confidenciales, nadie quiere intrusos. Para esta clase de tareas hay algunos protocolos especiales que permiten transmisiones de datos seguras y confidenciales.

- Uno de estos protocolos es ***Private Communications Technology***, que emplean algunos proveedores para las tiendas virtuales. Lo mejor es que active la opción *PCT 1.0*, para poder emplear esta tecnología en caso de duda.
- Active sin falta también las opciones *Use SSL 2.0* y *Use SSL 3.0*. Los ***Secure Socket Layers*** son el estándar de facto para una transmisión de datos segura en la Red. Algunos proveedores aún siguen empleando la versión antigua SSL 2.0.
- ***Transport Layer Security*** (TLS 1.0) es un estándar de seguridad abierto comparable a SSL 3.0 (ver más arriba). Hay que activar la opción Use TLS 1.0 si se desea que Internet Explorer transmita datos con esa tecnología.
- *Fortezza* es un sistema que permite a los usuarios identificarse ante un servidor web mediante tarjetas electrónicas. Pero hasta la fecha, esta tecnología altamente fiable basada en hardware se emplea casi exclusivamente en los Estados Unidos, por lo que en España podemos renunciar a esta función.

Recomendación: lo mejor es que active todos estos protocolos a excepción de Fortezza, ya que favorecen la seguridad. Aunque sólo se empleen de vez en cuando, no repercutirán negativamente en el rendimiento del navegador.

El asistente para perfiles

El asistente para perfiles es un módulo de Internet Explorer que le ayuda a la hora de administrar y transmitir datos personales. Facilita la comunicación de los datos empleados con frecuencia y al mismo tiempo, permite controlar quién debe recibir esa información. Si quiere emplear el *asistente para perfiles*, active la opción

Habilitar el asistente para perfiles. Si no lo quiere usar de ninguna manera, debería desactivar dicha opción. Así, evitará que el asistente para perfiles intervenga automáticamente en situaciones en las que pueda resultar molesto.

Recomendación: actívelo.

Redirección de los datos de formularios

Los formularios de entrada en las páginas web siempre suponen un peligro, sobre todo si hay que dar información confidencial como los datos de la tarjeta de crédito. Una técnica muy apreciada por los hackers es dirigir las entradas hechas por el usuario en formularios web interactivos desde el servidor original al suyo, para leerlas allí (más información en el Capítulo 1). Por esta razón, marque la opción *Advertir si el envío de formularios está siendo redirigido.* Así, Internet Explorer le advertirá de estos ataques.

Recomendación: ¡activar sin falta!

Las funciones de seguridad de Netscape Navigator

Desgraciadamente, Netscape Navigator no dispone de un concepto de seguridad tan amplio y sofisticado como el de Internet Explorer. Pero esto no quiere decir que sea menos seguro. Simplemente no permite configuraciones tan completas y flexibles. En lugar de esto, existen unas pocas opciones que regulan cuestiones básicas como el uso de Java o JavaScript. Pero habría que decir a favor de Netscape Navigator, que desiste totalmente del soporte de una tecnología tan cuestionable, desde el punto de vista de la seguridad, como ActiveX. De este modo, muchos agujeros de seguridad están cerrados desde el principio. Además, con Netscape no se producen ni con mucho interacciones peligrosas con el sistema operativo y otras aplicaciones. En este aspecto, aventaja claramente a Internet Explorer, con su interdependencia con los sistemas operativos de Windows y quizá con las aplicaciones Office de Microsoft.

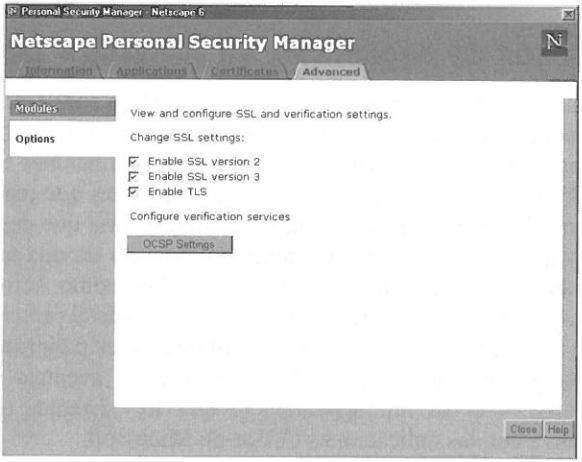
Aparte de esto, Netscape Navigator dispone de un sistema de certificado que permite verificar mediante certificados la autenticidad y fiabilidad de las páginas web. Aunque hasta la fecha estos certificados apenas se han impuesto, por lo que no ofrecen suficiente protección ante los contenidos destructivos. A continuación, les vamos a presentar las configuraciones y opciones de seguridad fundamentales de Netscape Navigator.

Activar los protocolos de cifrado

Netscape Navigator también puede realizar transmisiones de datos cifrados con servidores web, si lo requieren aplicaciones críticas como por ejemplo la banca electrónica y las tiendas virtuales, o la lectura de correo electrónico mediante

navegador web. En este aspecto, domina el cifrado por *Secure Socket Layers* (SSL). Pero para que realmente emplee estos protocolos en caso de necesidad, tendrán que haber sido activados. Esto es algo que usted debería verificar sin falta y, si fuera necesario, realizar la activación.

1. Para hacerlo, abra con *Taks/Privacy and Security/Security Manager* el administrador de seguridad de Netscape Navigator, que le permitirá realizar todas las configuraciones de este navegador que afecten a la seguridad.
2. Cambie ahora, en la barra de navegación superior, a la categoría *Advanced* (avanzadas) y a continuación, active en el margen izquierdo de la ventana el apartado *Options* (opciones).
3. Aquí encontrará tres opciones: *Enable SSL version 2*, *Enable SSL Version 3* y *Enable TLS* (Activar SSL Versión 2, activar SSL Versión 3 y TLS). Para que el navegador pueda emplear el respectivo protocolo de cifrado cuando lo necesite, tendrán que estar activadas las tres opciones.



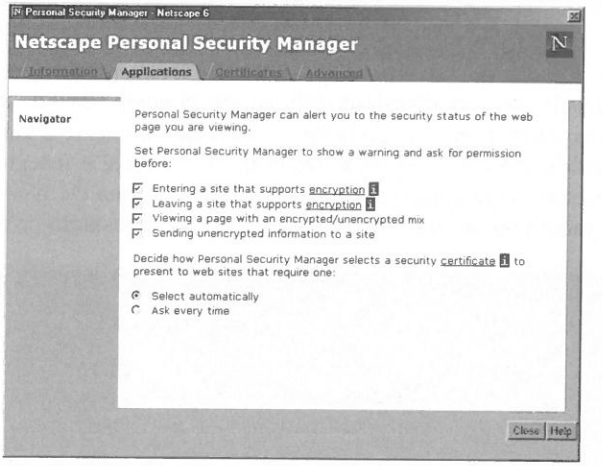
Aquí se activan los protocolos de cifrado en Netscape Navigator.

4. Después, haga clic sobre el botón *Close* (Cerrar) para guardar las configuraciones y salir del administrador de seguridad.

Dirigir conexiones seguras

El empleo de conexiones seguras con transmisión de datos cifrada sólo tiene sentido si podemos confiar ciegamente en que, por sistema, el navegador sólo transmita datos confidenciales codificados. Netscape Navigator tiene algunas configuraciones que permiten dirigir el comportamiento del navegador en situaciones críticas. De esta forma, se pueden activar por ejemplo advertencias, con las que el programa avisa al usuario de posibles riesgos.

1. Abra de nuevo con *Taks/Privacy and Security/Security Manager* (Tareas/Entorno privado y seguridad/Administrador de seguridad) el administrador de seguridad de Netscape Navigator.
2. Una vez dentro, cambie en la barra de navegación superior a la pestaña *Applications* (Aplicaciones). Encontrará una serie de opciones que dirigen el comportamiento del navegador en diferentes situaciones.



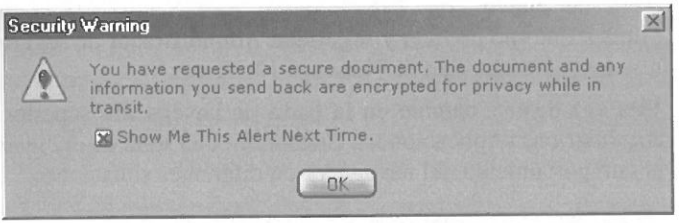
Estas opciones controlan las advertencias con las que Netscape Navigator avisa a sus usuarios.

3. *Entering a site that supports encryption* (activar una página web que soporte cifrado) hace que usted sea advertido expresamente del cambio de una conexión normal e insegura a una transmisión cifrada y segura. En este caso, Netscape Navigator visualizará una ventana de advertencia que tendrá que confirmar con *OK* o *Aceptar*. Desde ese momento, podrá introducir datos confidenciales como contraseñas, claves electrónicas, PINs, etc. sin que los puedan espiar terceros no autorizados.

TRUCO

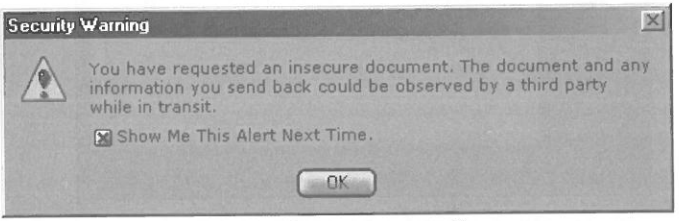
Confianza y confidencialidad

Una conexión segura aún no garantiza que sus datos confidenciales no vayan a parar a manos equivocadas. Los datos siempre son transmitidos al servidor web (aunque cifrados). Una vez allí podrán ser desencriptados y analizados por el operador, cosa que normalmente es lo que se pretende. Pero que un operador favorezca una transmisión de datos segura, no quiere decir que sea digno de confianza. Por ello, debería vigilar siempre al operador de una página web, sobre todo si es un proveedor pequeño y desconocido.



Así advierte Netscape Navigator del cambio a un modo de transmisión seguro.

4. Si activa la opción *Leaving a site that supports encryption* (salir de una página web que soporte cifrado), Netscape también advierte del caso contrario, es decir, si al salir de la banca electrónica vuelve a cambiar de una transmisión cifrada y segura a una conexión normal e insegura. También, en este caso, se le comunicará mediante una ventana de aviso que a partir de ese momento las entradas confidenciales ya no estarán protegidas.

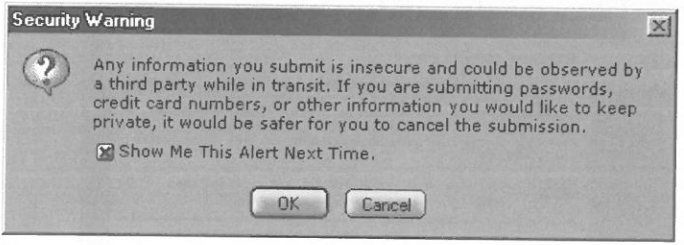


Este mensaje aparece al abandonar una conexión segura.

5. *Viewing a page with an encrypted/unencrypted mix* (visualizar una página web con información mixta - cifrada y no cifrada) se refiere a la situación, poco frecuente e insólita, de que una página web contenga también elementos inseguros. Esto puede ocurrir si, por ejemplo, una página está compuesta por varios bloques, que son cargados desde diferentes servidores de los cuales no todos soportan el cifrado. En la práctica, esto ocurre muy pocas veces y se suele deber a problemas técnicos (como por ejemplo dificultades en la transmisión). Pero, si al entrar por primera vez en una página nueva se encuentra con esta situación, sería recomendable que se tome en serio la ventana de aviso de Netscape Navigator y eche un vistazo a fondo.

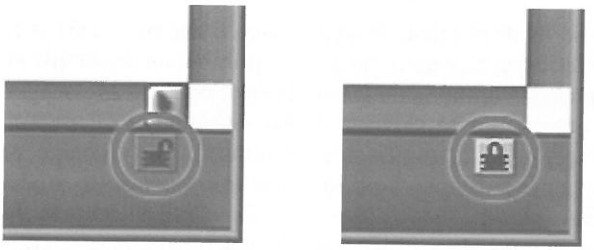
6. La opción *Sending unencrypted information to a site* (enviar información no cifrada a un sitio web) se encarga de advertirle cada vez que quiera transmitir datos de formulario a una página web sin que la transmisión pueda ser cifrada. Como estas transmisiones inseguras pueden ser espiadas, resulta muy arriesgado transferir de este modo datos confidenciales como contraseñas o información sobre la tarjeta de crédito. En este caso, podrá

hacer clic sobre *Cancel* (Cancelar) para impedir esa transmisión no protegida. Si prefiere correr el riesgo, prosiga con el botón *OK*.



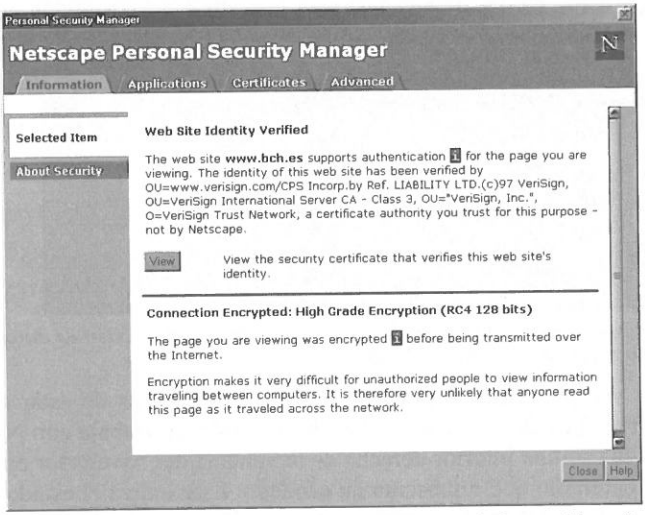
Netscape Navigator también puede avisar antes de la transmisión de datos de formulario a través de conexiones inseguras.

Aparte de las ventanas de aviso, existe otra posibilidad más de estar siempre informado sobre el estado de seguridad de la conexión. Si trabaja con Netscape Navigator, en la esquina inferior derecha de la ventana del navegador encontrará un pequeño símbolo que representa un candado. Éste indica el estado actual. Si es gris y la manija del candado está abierta, significa que la conexión es insegura y no va cifrada. Si por el contrario, el candado está cerrado y va reproducido en azul sobre fondo ámbar, la conexión será segura y usted podrá transmitir con toda tranquilidad información confidencial.



En la línea de estado, Netscape Navigator advierte sobre la inseguridad (izquierda) o seguridad (derecha) de las conexiones.

Si quiere saber más sobre la calidad de una conexión, en lo que a materia de seguridad se refiere, active el administrador de seguridad haciendo clic con el mouse sobre el símbolo del candado. Éste analizará el certificado de seguridad que ha transmitido el servidor web para esa conexión y resumirá para usted los datos más importantes. Aquí, se debería verificar si el certificado fue realmente emitido para esa página web, qué sistema de cifrado posee y si procede de un certificador digno de confianza. Vigile que la información crítica, como la que interviene en las transacciones de banca electrónica y similares, vaya protegida a ser posible por un cifrado de 128 Bit. Este cifrado es considerado en la práctica como seguro, mientras las claves menores, de hecho, han sido desencriptadas ya.



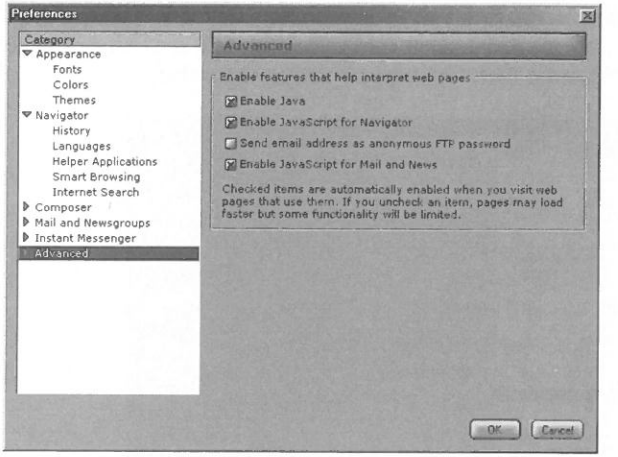
En el administrador de seguridad puede obtener información más detallada sobre la seguridad de la conexión.

Proteger la dirección de correo electrónico

Cuando tiene lugar el inicio de sesión para transferir archivos a través de FTP anónimo, Netscape Navigator tiene la costumbre de transmitir una dirección de correo electrónico extraída de las configuraciones de Messenger. Esto se debe, principalmente, a que la mayoría de los servidores FTP anónimos exigen una dirección de correo electrónico como contraseña. Sin embargo, una información tan valiosa como la propia dirección de correo electrónico no debería ser entregada con tanta alegría. Esto se lo pondría muy fácil a hackers o coleccionistas de direcciones, que podrían aprovechar este truco para hacerse con las direcciones de correo electrónico de sus víctimas. Existe una opción para quitarle esta fea costumbre a Netscape Navigator. Le recomendamos que verifique urgentemente esta configuración y, si fuera necesario, la desactive.

1. Para tal fin, abra mediante la secuencia de menú *Edit/Preferences...* las preferencias generales de Netscape Navigator.
2. Una vez dentro, seleccione en la parte izquierda de la barra de navegación, la categoría *Advanced* (Ampliado).
3. Esto hará que aparezcan en la mitad derecha de la ventana una serie de opciones, todas de vital importancia para la seguridad. Las opciones para Java y JavaScript controlan "si está permitido que las páginas web empleen estas tecnologías". Más adelante en este mismo capítulo, explicaremos esto con más detalle.

4. Para proteger la dirección de correo electrónico sirve la función *Send email address as anonymous FTP password* (enviar la dirección de correo electrónico como contraseña FTP anónima). Esta opción debe estar DESACTIVADA indudablemente, para que Netscape Navigator no "largue" su dirección de correo electrónico a cualquier servidor FTP que pase por ahí.



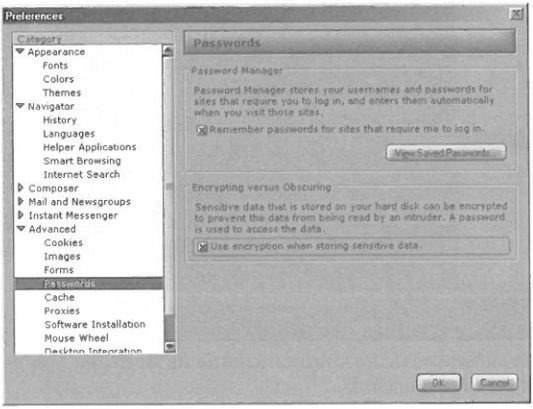
En el apartado Advanced de las configuraciones de Netscape Navigator, encontrará diversos ajustes de seguridad.

5. Guarde la opción modificada haciendo clic sobre el botón *OK*.

Proteger las contraseñas guardadas y las entradas de formularios

Netscape Navigator dispone de una serie de funciones "cómodas" que pueden automatizar y así acelerar los arranques de sesión y las entradas de formularios que se hagan con regularidad. Esto resulta agradable y cómodo, pero no está del todo exento de peligro. Si por ejemplo, usted permite que al conectarse a una página web su contraseña sea introducida automáticamente, cualquiera que tenga acceso a su PC también podrá aprovechar esta aplicación automática, recibiendo así acceso a los datos confidenciales. Para cerrar este agujero de seguridad y seguir facilitando toda la comodidad posible, Netscape Navigator puede guardar, cifrados, todos los datos que sean relevantes para la seguridad. Si durante una sesión de Internet usted quiere acceder a los datos así almacenados, sólo tendrá que hacer una única introducción de contraseña para liberar, mientras dure esa sesión, todos los datos almacenados. Al cerrar Netscape Navigator se restablecerá automáticamente la protección, de modo que en su ausencia nadie pueda hacer mal uso de las funciones confort del navegador.

1. Para activar esta función protectora, acceda a las preferencias generales de Netscape mediante la secuencia de menús *Edit/Preferences...*
2. Despliegue en la parte izquierda de la barra de navegación la categoría Advanced y seleccione la subcategoría *Passwords* (Contraseñas).
3. A continuación, verá en la zona inferior de la mitad derecha de la ventana el área *Encrypting versus Obscuring* (Cifrar y ocultar), donde podrá activar la opción *Use encryption when storing sensitive data* (emplear cifrado al guardar datos relevantes para la seguridad).



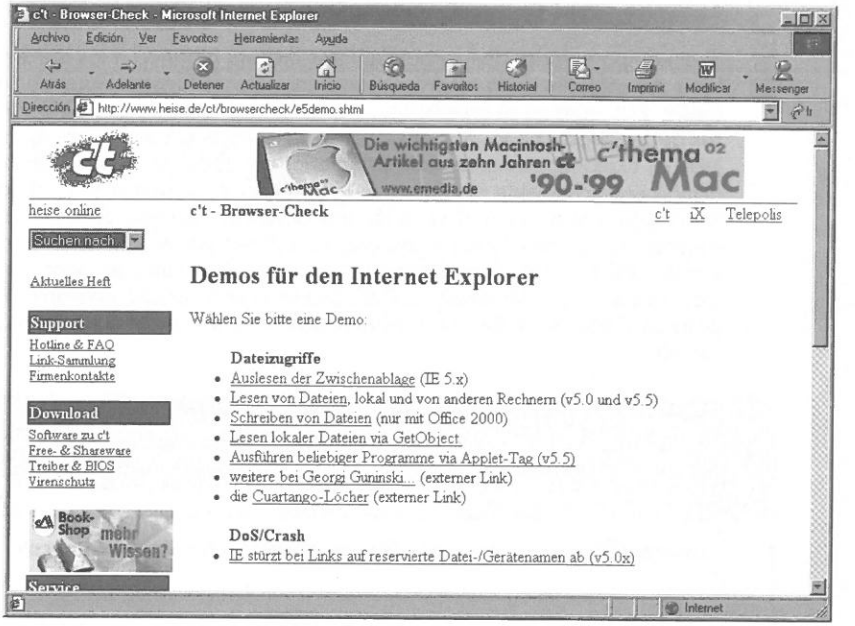
Active en Netscape Navigator el almacenamiento cifrado de los datos relevantes para la seguridad.

4. Confirme las nuevas configuraciones haciendo clic sobre *OK*.

Peligros causados por agujeros de seguridad

Los mejores conceptos y funciones de seguridad no sirven de nada si no se implementan correctamente. Desgraciadamente, cuando se desarrolla software, los errores están a la orden del día y productos tan complejos como los navegadores web no son precisamente la excepción. Muchas veces, estos errores de programación no tienen por qué originar necesariamente un mal funcionamiento o una caída del sistema. Más bien suelen manifestarse de manera mucho más discreta y peligrosa. Por ejemplo, un programa defectuoso de un intérprete de JavaScript en Internet Explorer puede tener como consecuencia que una página web tenga permiso para ejecutar funciones script que, según el concepto de seguridad, no debería realizar. Si usted quiere convencerse de los agujeros de seguridad existentes y de si afectan a su PC, le recomendamos el browser check que ofrece, en alemán, la revista *c't* bajo la dirección:http://www.heise.de/ct/browsercheck/demos.shtml. Con él, podrá testear una serie de conocidos aguje-

ros de seguridad, tanto para Netscape Navigator como Internet Explorer. Naturalmente, este programa está "descafeinado", es decir, no podrá causar la destrucción de archivos u otras pérdidas de datos. Pero cuando haga la prueba, sí que debería contar con la caída del navegador o del ordenador. Por esta razón, las pruebas se hacen a propio riesgo y deberían ser emprendidas con cuidado.



Bajo http://www.heise.de/ct/browsercheck/e5demo.shtml , podrá testear los agujeros de seguridad de Internet Explorer.

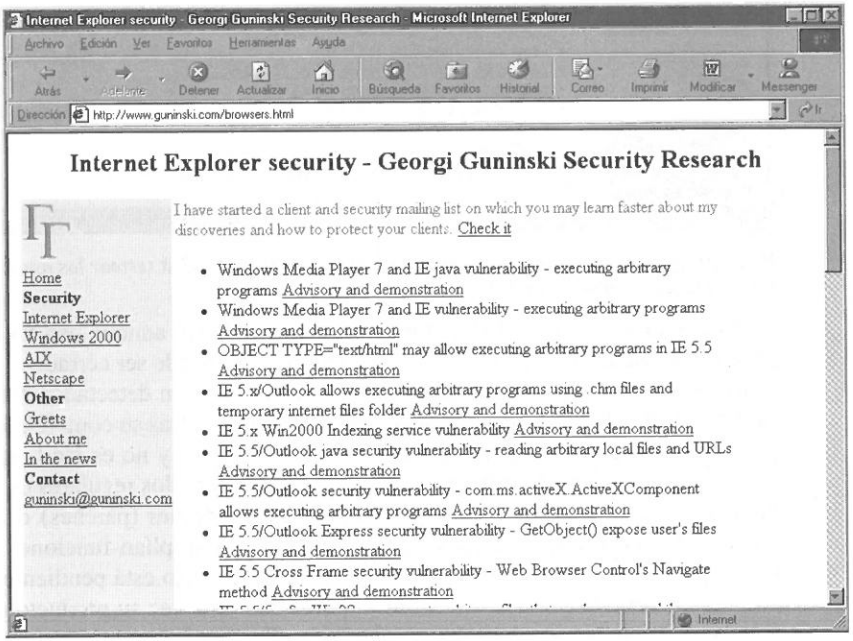
Estos agujeros de seguridad suponen un grave peligro, aunque eso ya se desprende del hecho de que un agujero de este tipo sólo puede ser cerrado si ha sido descubierto. Como muchos agujeros de seguridad no son detectados durante la fase de prueba de una nueva versión, sino que aparecen tras su comercialización, para entonces el software ya está en manos del usuario y no es fácil repararlo. Por eso las empresas de software comercializan a intervalos regulares de tiempo paquetes suplementarios de sus productos. Estos *Patches* (parches) o *Service Packs* corrigen los errores detectados a posteriori o amplían funciones importantes ya existentes. Pero esto sólo funciona si el usuario está pendiente y solicita dichas actualizaciones. Un usuario que instale una vez su producto de software y ya no se preocupe del mantenimiento, queda totalmente a merced de los agujeros de seguridad.

Por ello, es muy importante mantenerse siempre al corriente sobre el estado de seguridad del propio software y realizar cuanto antes las actualizaciones que afecten a la seguridad. Una buena fuente para obtener información actualizada sobre los agujeros de seguridad puede ser la página web de Georgi Guninski bajo la dirección: http://www.guninski.com.

INFO

Georgi Guninski – la pesadilla de Bill Gates

Si el equipo creador de Internet Explorer disfruta jugando a los dardos a la hora del café, sin duda tendrá pegada una foto de Georgi Guninski sobre la diana. Este hombre se cree llamado (encomiable tarea) a descubrir los agujeros de seguridad de los navegadores web. Cosa que hace, sobre todo en Internet Explorer, con gran éxito por cierto; de modo que a intervalos de tiempo pasmosamente regulares, es fácil ver en los tickers alguna noticia sobre agujeros de seguridad recién descubiertos. Guninski documenta en su página web los problemas y agujeros detectados por él y también por otros, dando casi siempre algún consejo sobre cómo eliminarlos en poco tiempo. Cabe esperar que Microsoft contrate pronto a esta cabeza pensante. Pero no para acallarla, sino para que sus productos tengan desde el principio mejor aspecto.



Bajo la dirección http://www.guninski.com/browsers.html puede encontrar información actual sobre los agujeros de seguridad.

Active Setup – actualizar Windows e Internet Explorer

Microsoft ofrece a través de Internet un "update" o actualización para sus productos. Active Setup le permite verificar directamente en la página web de Microsoft las correcciones de errores y ampliaciones de función disponibles. El proceso analiza el software instalado en el PC, de modo que sólo se proponen las actualizaciones realmente necesarias.

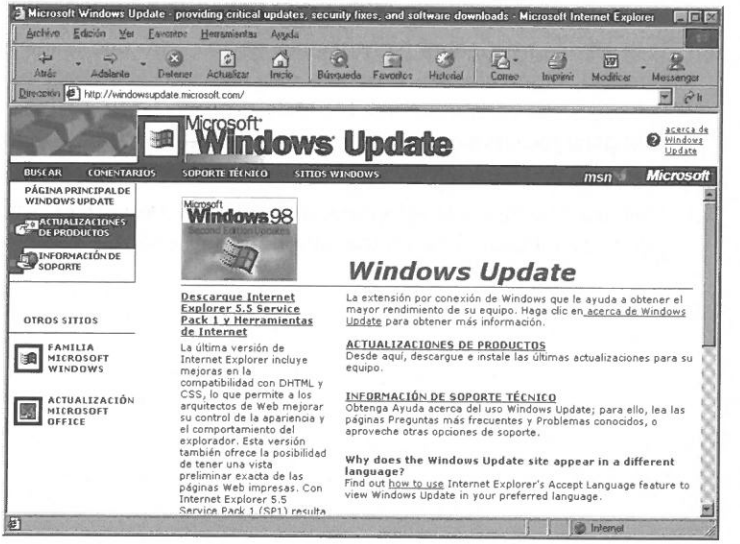
1. Para utilizar Active Setup, active en el menú inicial de Windows la opción *Inicio/Windows Update*. Esto arranca Internet Explorer y lo dirige a la página web de actualizaciones de Microsoft.
2. Arranque en *Actualizaciones de productos* el componente ActiveX que analizará su PC y le hará sugerencias sobre las actualizaciones posibles.

TRUCO

Update sólo con ActiveX

Importante: Para que el update funcione, primero tendrá que liberar en las configuraciones de seguridad la ejecución de elementos ActiveX (al menos, temporalmente).

3. Marque los updates que desee en la lista de actualizaciones. Por supuesto, sería recomendable seleccionar todo lo que tenga que ver de algún modo con la seguridad (updates de seguridad).



Windows e Internet Explorer pueden (y deberían) ser actualizados continuamente a través de Internet.

4. Una vez cerrada la selección, comience la transmisión haciendo clic sobre la flecha *Download*. Ahora tendrá lugar la instalación online de todos los componentes indicados. Después de este proceso, generalmente hay que reiniciar el ordenador.

INFO

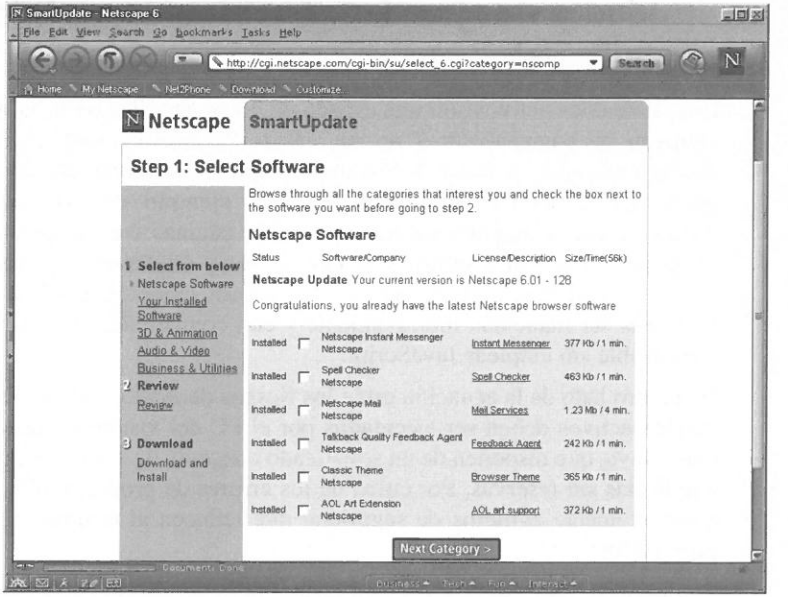
¿Espía Microsoft a sus clientes?

Funciones como Active Setup causan constantes confusiones a los clientes y quejas de los protectores de datos. En principio, el análisis del software existente resulta conveniente, para poder hacer al cliente sugerencias individuales sobre las actualizaciones. Pero los datos así obtenidos, también pueden ser guardados perfectamente para crear un perfil y aprovechados posteriormente. Microsoft afirma (también en relación con Active Setup) que no almacena los datos... ¡bueno! Sin embargo, la siguiente reflexión podría servir en defensa de Microsoft: si uno sólo ha instalado en su PC software con licencia pagado religiosamente, no tiene nada que ocultar, ¿verdad?

SmartUpdate – actualizar Netscape Navigator

También Netscape ha desarrollado una función de actualización online para Navigator. Con *SmartUpdate*, usted puede completar Netscape Navigator a través de Internet con las correcciones de errores y ampliaciones importantes.

1. Para actualizar Netscape Navigator y sus componentes, active la página web de SmartUpdate bajo la dirección http://www.netscape.com/smartupdate y desde allí, arranque la actualización.
2. Esta página averiguará las versiones de software que tenga en su PC y le ofrecerá, según el caso, versiones más nuevas o actualizaciones. Para cada actualización encontrará una breve descripción (*Description*), que le explicará para qué sirve cada update. Si desea realizar una actualización, marque la casilla correspondiente en la lista.
3. Una vez finalizada la selección, avance hasta *Download*. Ahora, los componentes solicitados serán transmitidos e instalados.



Con SmartUpdate (http://www.netscape.com/Smartupdate) usted puede actualizar Netscape Navegator.

3.3 Un PC teledirigido – los peligros de ActiveX, JavaScript & Co.

En los comienzos de la Red, las páginas web se componían sólo de texto e imágenes. Comparado con lo que se conocía hasta entonces, eso ya suponía un progreso tremendo y todo el mundo estaba contento. ¡Pero no por mucho tiempo! A fin de cuentas, siempre queremos que todo sea más colorido, más excitante y más dinámico. Así que, hubo que ampliar la Red con contenidos activos (en contraste con los textos e imágenes inmóviles). Éstos son programas que no se ejecutan en el servidor web, sino en el ordenador del visitante, por lo que tienen un acceso más o menos limitado a sus recursos y archivos. Y en ese "más o menos" es donde radica el problema. Mientras algunos tipos de componentes activos son relativamente seguros, otros abren las puertas de par en par a los abusos. A continuación, le vamos a mostrar las clases de contenidos activos que hay, hasta dónde son seguros y cómo protegerse de los peligros que originen.

Utilidad y riesgos de los contenidos activos en páginas web

Los contenidos activos son una espada de doble filo. Por un lado, animan enormemente las páginas web. Y no me refiero únicamente al atractivo visual, sino también a la gran variedad de funciones y aplicaciones que sólo con texto e imágenes serían impensables. Un excelente ejemplo de esto es JavaScript. Actualmente, la mayoría de los autores de páginas web emplean el lenguaje script para desarrollar sistemas de navegación y asistentes, además de ponérselo más fácil al usuario. Una página web extensa, compleja y que al mismo tiempo pueda ser manejada intuitivamente y con comodidad, resulta prácticamente impensable sin emplear JavaScript.

En el otro lado de la ecuación están los riesgos derivados del hecho que los contenidos activos deben ser ejecutados por el PC del visitante. Hasta tecnologías como Java, que disponen de un sofisticado concepto de seguridad, no pueden ser empleadas sin reservas. Por culpa de los errores de programación, se producen constantemente agujeros de seguridad que reducen al absurdo el concepto de protección.

Precisamente por esa dificultad en encontrar el equilibrio entre estos dos aspectos, comodidad y seguridad, muchos usuarios ignoran el problema atendiendo al lema "a mí no me va a afectar". Pero este enfoque es muy peligroso. Además, los contenidos activos pueden ser usados también con seguridad, si se aprovechan las posibilidades de los navegadores web y el correspondiente software de protección, como vamos a demostrar en las páginas siguientes.

¿Qué daño pueden causar los contenidos activos?

Como ya se ha explicado anteriormente, los contenidos activos se ejecutan en el PC del visitante. Esta es la diferencia fundamental con respecto a contenidos estáticos, como son las páginas web sencillas con textos e imágenes. Estas últimas, sólo son datos que visualiza el navegador web, pero los contenidos activos son instrucciones que ejecutan el navegador o los intérpretes especiales. Por lo tanto, según sean estas instrucciones, los componentes activos teóricamente podrían ejecutar todas las funciones del ordenador.

Aplicado a la práctica, esto no es en absoluto una exageración. Por ejemplo, un control ActiveX puede hacer todo lo que podría ejecutar cualquier programa de Windows. Incluso acceder a todos los archivos en modo de lectura y escritura, activar cualquier hardware existente, formatear discos duros, etc. Otros componentes activos en Java o JavaScript están sometidos a restricciones, pero también aquí se detectan constantemente nuevos agujeros de seguridad y trucos, que bien sirven para hacer un uso ilícito de estas técnicas. Por lo que se debe tomar muy en serio el peligro que emana de los contenidos activos.

Desactivación fiable de los componentes ActiveX

Mejor será que empecemos por el más peligroso, para que usted lo pueda desactivar el primero, si fuera necesario: *ActiveX* es la respuesta de Microsoft a la amenaza representada por *Java*, el lenguaje de programación independiente de plataformas que se impone más y más en Internet y está poniendo en apuros al monopolio de Microsoft. Actualmente, el propio Microsoft ya ha desechado esta tecnología y se ha subido al tren de Java. Pero las versiones existentes de Internet Explorer llevan integrado ActiveX, por lo que el usuario tiene que ver cómo se las arregla con él. Entonces, ¿en qué consiste todo esto?

Los componentes ActiveX son programas ejecutables que van unidos a páginas web. De este modo, pueden ser difundidos a través de una red como por ejemplo Internet. El usuario llama a la correspondiente página web, el navegador carga la página con los componentes pertinentes y la ejecuta. Estos componentes pueden ser generados, por ejemplo, con VisualBasic (por supuesto, también de Microsoft). Lo más chocante de todo es que los componentes ActiveX entran directamente en el PC del visitante como programas binarios. Esto trae consigo buenas y malas noticias:

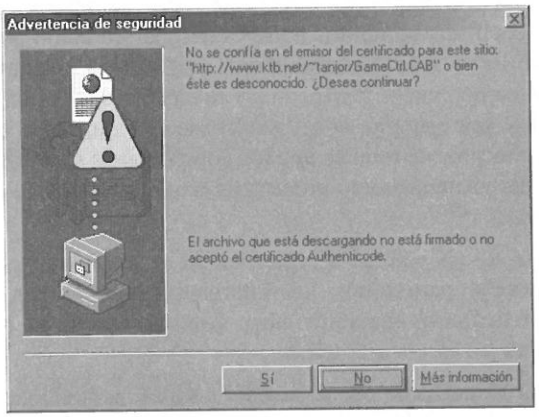
- Los componentes ActiveX sólo se ejecutan en PCs con Windows. Hasta aquí, la buena noticia para todos los internautas que tengan Linux, Macintosh, Unix, BeOs o cualquier otro sistema operativo ajeno a Windows. A ellos no les afecta este tema.
- Como un programa VisualBasic puede acceder a todas las funciones de un PC bajo Windows, esto regirá también para un componente ActiveX creado con VisualBasic. El navegador no controla en absoluto las funciones concretas que ejecute este componente. Le transfiere todo el control sobre el PC.
- Ahora bien, lo que haga un componente ActiveX con exactitud, es algo que sólo puede saber su programador. Da igual que invite a una agradable ronda de Tic Tac Toe, instale un troyano en su PC o reformatee su disco duro. Usted no lo sabrá hasta que no ejecute ese componente.

Para centrarnos en el tema: ejecutar un componente ActiveX, es algo así como bajarse de Internet cualquier programa Windows y arrancarlo sin haberlo sometido a ningún control antivirus u otra medida de precaución, sólo para ver lo que hace. No hay que extrañarse si después, resulta que el disco duro está vacío.

Componentes ActiveX certificados por Authenticode

Hasta Microsoft se vio obligado a reconocer las ostentosas deficiencias de seguridad de la tecnología ActiveX. Por lo que desarrolló bajo el nombre *Authenticode* un mecanismo de seguridad, mediante el cual los componentes

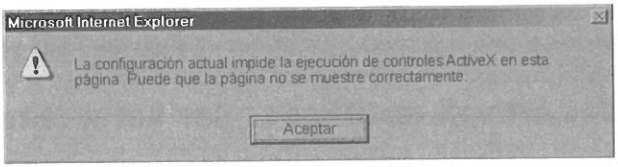
ActiveX reciben un certificado por parte de una entidad independiente. Éste es presentado al usuario cuando descarga el componente para confirmar su inocuidad. Pero desgraciadamente, su utilidad es limitada, ya que se ha demostrado que incluso componentes ActiveX absolutamente destructivos no tienen problemas a la hora de conseguir un certificado hasta del propio Microsoft. Además, precisamente muchos programadores aficionados no se pueden permitir solicitar un (costoso) certificado para cualquiera de los pequeños componentes cuya finalidad sea animar su propia homepage. En estos casos, Internet Explorer suele advertir al usuario lapidariamente de que no hay certificado y le deja solo ante la decisión.



En caso de componentes ActiveX sin certificado, sólo aparece un mensaje lapidario.

Protección contra los componentes ActiveX

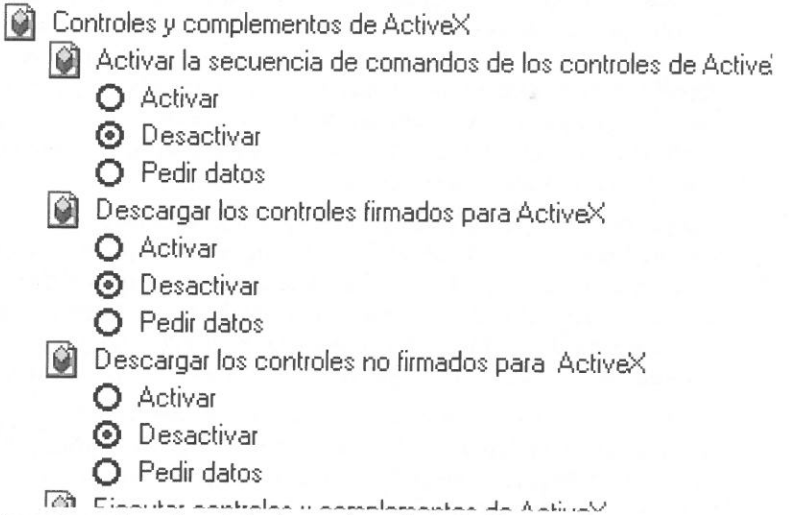
La mejor protección contra ActiveX es ignorarlo. Olvide simplemente que los componentes ActiveX existen. Eso lo logrará configurando Internet Explorer para que rechace de plano la descarga y ejecución de los componentes ActiveX. Así, si usted carga una página web con un contenido ActiveX, Internet Explorer le advertirá de que esa página no puede ser visualizada correctamente a causa de las configuraciones de seguridad.



Sí se puede estar sin él: al renunciar a ActiveX, pueden aparecer de vez en cuando mensajes de error.

Si confirma la advertencia, se encontrará con una gran interfaz vacía en lugar del componente. Pero la ventaja es que ya no deberá preocuparse de los posibles peligros.

1. Para desactivar ActiveX en Internet Explorer, abra con *Herramientas/Opciones de Internet...* la categoría *Seguridad* que contiene las configuraciones de seguridad.
2. Elija la zona de seguridad para la que quiera impedir la ejecución de los componentes ActiveX, como por ejemplo *Internet*.
3. En ninguno de los niveles de seguridad predefinidos se desactiva del todo la ejecución de componentes ActiveX. Por ello, para ActiveX no importa en principio el nivel de seguridad predeterminado que usted elija. Aunque lo mejor es que conserve la configuración estándar. Después, haga clic sobre el botón *Personalizar nivel*.
4. Busque en la lista de configuraciones la entrada *Controles y complementos de ActiveX* y *desactive* todas las opciones que dependan de ActiveX.



Lo mejor es desactivar todas las opciones de ActiveX.

5. Con esto, queda impedida la ejecución de todas las funciones ActiveX. Confirme las nuevas configuraciones dos veces con *Aceptar*.

ActiveX en otros navegadores

Quien utilice otro navegador que no sea Internet Explorer, no debe preocuparse por ActiveX. IE es el único navegador que soporta esta tecnología (en realidad,

propiedad de Microsoft). Para Netscape Navigator existe un plug-in que permite habilitar también ActiveX. Pero en vista de los agujeros de seguridad descritos, ¿quién va a querer hacerlo?

TRUCO

Si a pesar de todo resulta imprescindible...

Si usted necesita a toda costa utilizar una página web que incluya componentes ActiveX y está seguro de que no es peligrosa, naturalmente deberá hacerlo. Pero no por ello desactive de golpe todas las configuraciones ActiveX para todas las páginas web. En su lugar, aproveche el concepto de seguridad de Internet Explorer y asigne esta página web a la zona de seguridad para sitios dignos de confianza. Para esa zona, podrá permitir la utilización de componentes ActiveX.

Impedir la ejecución de Java-Applets

Java es una de las grandes leyendas de éxito en Internet. En muy pocos años, este lenguaje de programación multiplataforma se ha impuesto en todo el mundo. El término multiplataforma significa que un programa Java, una vez escrito, puede ejecutarse en cualquier ordenador. Es decir, tanto en un PC bajo Windows como en un ordenador Linux, una workstation Unix o un teléfono móvil WAP. Por ello, los programas JAVA resultan indicados para unirlos a páginas web que puedan ser llamadas desde los más diversos ordenadores. Esto lo aprovechan por ejemplo muchos bancos online, uniendo su software de banca a una página web como Java-Applet.

Para garantizar esta independencia de plataformas, los programas Java no son difundidos en forma de código binario como los programas normales (ya que este debería ser adaptado especialmente a cada sistema operativo), sino en un formato intermedio, el Bytecode. Éste es recibido en el ordenador objetivo por una máquina de Java virtual, que transforma el bytecode independiente de plataformas en un *bytecode* específico que finalmente pueda ser ejecutado.

No tema, no pretendemos aburrirle ahora con detalles técnicos. Seguimos con el tema de la seguridad en Java. Y es que esta máquina virtual de Java permite garantizarla óptimamente. A fin de cuentas, el propio programa Java sólo puede ejecutar lo que le permita la máquina virtual de Java. Marcándole a ésta las restricciones oportunas, también podemos mantener a raya cualquier programa Java. En resumidas cuentas, la máquina virtual es algo así como una celda acolchada donde se pueden desfogar hasta los Java-Applets más malignos, sin llegar a causar daños en el ordenador.

¿Hasta qué punto resulta seguro Java?

Java dispone de un concepto de seguridad muy sofisticado, que garantiza ampliamente la seguridad de los datos locales en el PC del usuario. Este lujo se

debe a que Java (al contrario de ActiveX) no es sólo una técnica más para facilitar contenidos activos en la Red, sino un lenguaje de programación completo que permite crear hasta aplicaciones complejas. Esto hace que los requisitos de seguridad de origen sean mucho más exigentes. Así, existen algunas reglas a las que se deben atener todos los Applets. Los programas Java:

- Sólo pueden acceder a determinadas áreas del sistema de archivos local que hayan sido previamente definidas.
- No tienen permiso para activar otros programas dentro del ordenador.
- Sólo pueden establecer vínculos de red con el ordenador de Internet desde donde hayan sido cargados.
- Sólo pueden acceder al sistema de archivos local o intercambiar datos a través de la Red, pero jamás las dos cosas a la vez. Así, se pretende evitar que los Applets espíen a los usuarios.

Tampoco se permiten accesos directos a la memoria por parte de los programas. Antes de su ejecución, todas las instrucciones son verificadas por un administrador de seguridad de la máquina virtual de Java, que sólo las permitirá si no suponen ningún peligro potencial.

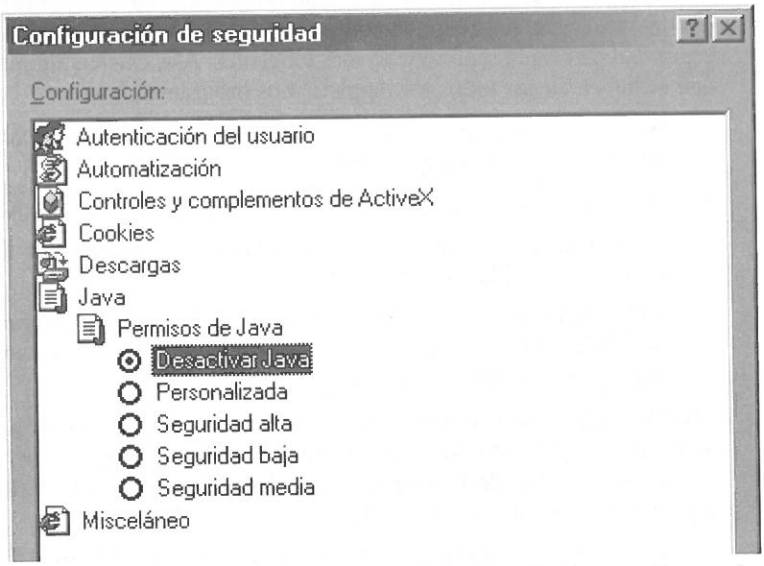
Aun así, también Java presenta riesgos atribuibles, sobre todo, a las implementaciones de las máquinas Java virtuales, según están incluidas por ejemplo en Internet Explorer y Netscape Navigator. Aquí, errores o negligencias de los programadores podrían dejar abiertas puertas traseras, que en algún momento podrían ser descubiertas y aprovechadas por los hackers. Aunque por otro lado, como para eso se requiere un mínimo de conocimientos y experiencia, se podría considerar a Java como relativamente seguro.

Desactivar Java en Internet Explorer

Si usted no quiere correr ningún riesgo, puede desactivar totalmente la ejecución de Java-Applets. En Internet Explorer, deberá proceder del siguiente modo:

1. Abra desde *Herramientas/Opciones de Internet...* la categoría *Seguridad*, donde vienen las configuraciones de seguridad de Internet Explorer.
2. Seleccione la zona de seguridad para la que quiera impedir la ejecución de Java-Applets.
3. Como ninguno de los niveles de seguridad predefinidos desactiva totalmente la ejecución de Java-Applets, puede dejar tranquilamente el nivel de seguridad estándar. Ahora, haga clic sobre el botón *Personalizar nivel...* .
4. Busque en la lista de configuraciones la categoría Java y dentro de ésta, la subcategoría *Permisos de Java*.

5. Seleccione la opción *Desactivar Java*.



Con esta opción puede desactivar la ejecución de Java-Applets para la zona de seguridad elegida.

6. Guarde las nuevas configuraciones de seguridad mediante *Aceptar*.

Aprovechar las zonas de seguridad de Internet Explorer

Sin embargo, sólo resulta realmente recomendable desactivar Java-Applets si usted es un fanático de la seguridad y está dispuesto a asumir las desventajas que esto trae consigo. Y es que cada vez hay más páginas web que emplean Java. Sobre todo en banca y bolsa electrónica, cada vez más de moda, se suelen emplear Java-Applets. Si desactiva Java, ya no podrá visitar estas páginas web, salvo que exista una oferta comparable a nivel HTML. Por esta razón, le recomiendo que a la hora de configurar la seguridad de Java, aproveche las zonas de seguridad de Internet Explorer. Aquí podrá desactivar Java para la zona Internet general, pero incluir las ofertas de su banca electrónica, por ejemplo, en la zona de sitios de confianza donde se permite la ejecución de Java-Applets. De este modo, consigue seguridad y comodidad con un nivel de riesgo justificable.

TRUCO

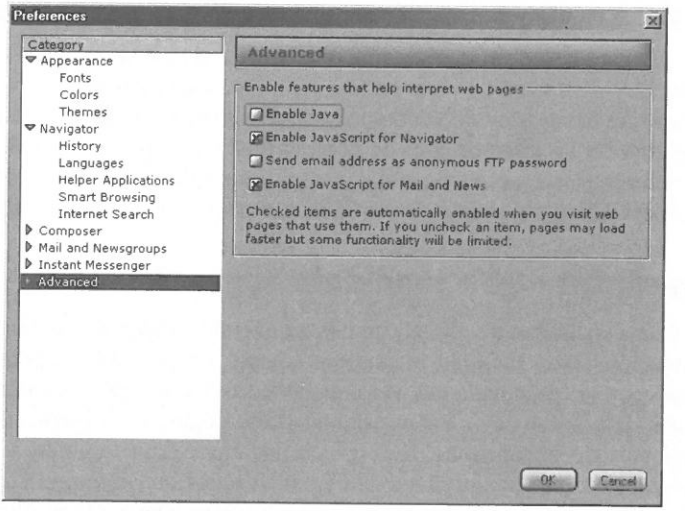
Protección contra contenidos activos mediante firewalls

Otras posibilidades de conseguir una protección flexible y fiable pueden ser los programas de protección especiales, como por ejemplo los firewalls o cortafuegos personales. Éstos pueden ser ajustados de modo que impidan la carga y ejecución de Java-Applets (y también de componentes ActiveX) o avisen al usuario, en cada caso, del posible peligro. Una solución especialmente flexible permite distinguir entre las páginas web. Es decir, sólo se permitirán los contenidos activos de determinadas direcciones mientras todas las demás serán cribadas automáticamente. En el siguiente capítulo, podrá consultar más información acerca de los firewalls personales.

Desactivar Java en Netscape Navigator

También Netscape Navigator permite desactivar la ejecución de Java-Applets. En realidad no ofrece ningún concepto de seguridad flexible equiparable al de Internet Explorer, de modo que Java sólo puede ser activado o desactivado. Si se quiere lograr una protección flexible, hay que recurrir obligatoriamente a software adicional del tipo firewalls personales.

1. Arranque Netscape Navigator y abra las opciones de este navegador mediante *Edit/Preferences*.
2. Cambie ahora a la categoría *Advanced*.
3. Ahora, vaya a la mitad derecha de la ventana y desactive la opción *Enable Java*.



Con esta opción evita la ejecución de Java-Applets en Netscape Navigator.

4. Confirme la modificación con el botón *OK*, para guardar las nuevas configuraciones definitivamente.

Peligros causados por scripts dinámicos

Otro tipo de contenidos activos son los scripts. Se trata de bloques de instrucciones relativamente cortos y sencillos que permiten manipular prácticamente todos los objetos del navegador web. Por objeto se entiende tanto el propio navegador web como sus distintos componentes (por ejemplo, la barra de estado), al igual que la página web representada. Los componentes incluidos en la página web como pueden ser apartados, imágenes, colores de fondo, hipervínculos, etc., son a su vez objetos que pueden ser tratados y modificados con instrucciones script. Esto proporciona al programador de scripts una variedad casi ilimitada de posibilidades para configurar dinámicamente las páginas web. Un ejemplo sencillo y muy conocido de aplicaciones script es lo que se suele llamar "MouseOver", donde la imagen, como puede ser un menú de selección, cambia cada vez que el puntero del mouse se desliza sobre ella. Pero existen muchas más posibilidades.

Frente a Java y ActiveX, los scripts tienen la ventaja de ser mucho más fáciles de aplicar. Incluso un programador de HTML aficionado que pretenda dinamizar un poco su homepage, con algo de paciencia y un cursillo de iniciación como los que se ofrecen regularmente en las revistas del sector, podría crear muy pronto sus propios scripts o adaptar los existentes a sus necesidades. Además, la tecnología de script permite emplear asistentes, con los que se pueden crear efectos dinámicos en páginas web sin tener que recurrir para nada a la programación.

Los scripts no son programas independientes, sino instrucciones que suelen ir integradas directamente en la página web. Para que estos scripts puedan ser ejecutados, el navegador web deberá soportar scripts, es decir, tendrá que ser capaz de reconocer las instrucciones e interpretarlas. Las versiones actuales de Internet Explorer y Netscape Navigator conocen el ampliamente difundido JavaScript. Internet Explorer asimila, además, VisualBasicScript, propio de Microsoft.

JavaScript – ¿Un candidato seguro?

Muchos consideran que JavaScript es una versión aligerada del lenguaje de programación Java. También el nombre sugiere un parentesco, pero en realidad JavaScript no tiene nada que ver con Java. Lo que tienen en común los dos lenguajes de programación es su orientación al objeto y, en cierto modo, la independencia de plataformas. Los programas JavaScript también se ejecutan en cualquier ordenador que disponga de navegador con intérprete de JavaScript. JavaScript fue desarrollado por la empresa Netscape y su nombre sólo puede deberse a un intento de promocionar este desarrollo independiente, al amparo de

la euforia general suscitada por Java. Y parece que con esta estrategia, Netscape acertó de pleno. Hoy en día, JavaScript ya es el lenguaje script reconocido en la Red y prácticamente todos los navegadores lo soportan en mayor o menor medida.

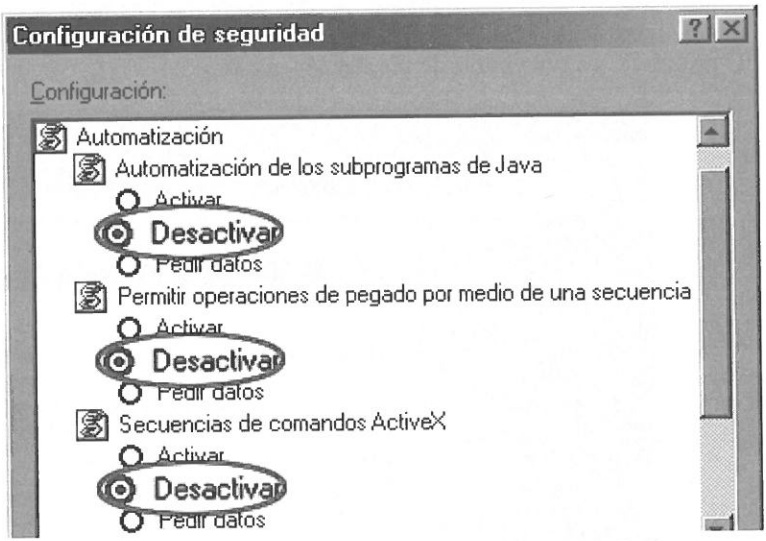
Una diferencia entre Java y JavaScript es el concepto de seguridad. Java tiene uno, JavaScript no. El lenguaje script más bien confía en el hecho de que al fin y al cabo, sólo facilita funciones de acceso a los objetos del navegador web, con lo que no puede salir de éste ni acceder a otras funciones del ordenador. Hasta aquí la teoría. En la práctica, resulta absolutamente posible hacer un uso ilícito de JavaScript. Por una parte, sirve para obtener información, ya que JavaScript permite averiguar multitud de datos sobre el software empleado por un usuario. Además, también es posible abusar del propio JavaScript, como mínimo para poner nerviosos a los visitantes de las páginas web. Por ejemplo, con Java Script se podrían abrir más y más ventanas del navegador nuevas, hasta que el ordenador del usuario se descontrolara o acabara colapsado del todo. En la dirección http://www.vippro.de/hirnbrauser pueden encontrar una página, en alemán, que sirve para probar las posibilidades que ofrece JavaScript y hasta qué punto su propio PC es susceptible de ser atacado por él.

Bajo http://www.vippro.de/hirnbrauser puede probar los agujeros de seguridad de JavaScript.

Desactivar JavaScript en Internet Explorer

Para evitar los riesgos causados por JavaScript, usted podrá impedir la ejecución de estas instrucciones. En Internet Explorer se hace del siguiente modo:

1. Abra las configuraciones de seguridad de Internet Explorer con *Herramientas/Opciones de Internet...* y desde allí, cambie a la categoría *Seguridad*.
2. Elija la zona de seguridad para la que quiera impedir la ejecución de scripts y haga clic sobre el botón *Personalizar nivel...*
3. Busque en la lista de opciones el apartado *Automatización*.
4. Desactive las opciones *Automatización de los programas de Java*, *Permitir operaciones de pegado por medio de una secuencia de comandos* y *Secuencias de comandos de ActiveX*, para evitar la ejecución de las instrucciones JavaScript.



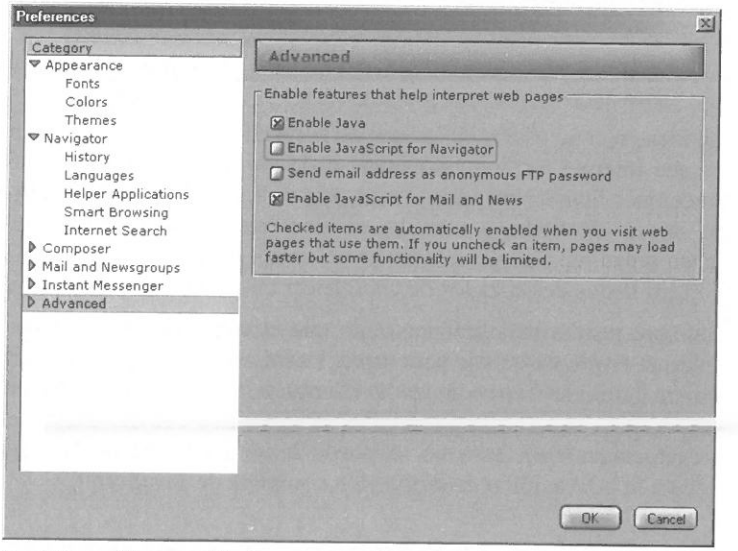
Con estas opciones evita la ejecución de JavaScript en Internet Explorer.

5. Guarde las nuevas configuraciones de seguridad con *Aceptar*.

Desactivar JavaScript en Netscape Navigator

Aunque Netscape haya desarrollado JavaScript, el navegador de la misma casa también ofrece la opción de impedir la ejecución de instrucciones JavaScript. ¿Es que no se acaban de fiar de su propia creación?

1. Arranque Netscape Navigator y desde *Edit/Preferences* abra las preferencias de Netscape.
2. Aquí, cambie a la categoría *Advanced*.
3. Desconecte la opción *Enable JavaScript for Navigator*.



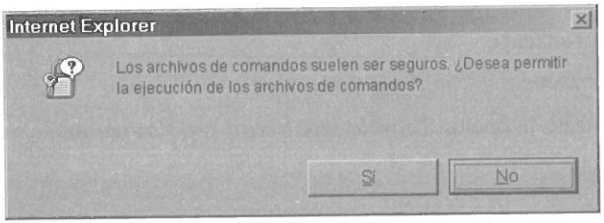
También en Netscape Navigator se puede desactivar JavaScript.

4. Confirme con *OK*.

¿Realmente se puede renunciar a JavaScript?

Hoy en día, JavaScript ha alcanzado tal popularidad que es empleada en muchas, muchísimas páginas web. Esto tiene un problema: a los autores de estas páginas no se les ha ocurrido pensar que sus visitantes pueden no ser tan amigos de JavaScript como ellos. Por eso, las páginas con JavaScript desactivado suelen ofrecer un aspecto bastante pobre, o incluso no servir para nada, ya que basan completamente su navegación en estos scripts. Por lo tanto, si no queremos ser excluidos desde un principio de estas páginas web, no podremos desactivar JavaScript sin más. ¿Qué hacer entonces?

Internet Explorer ofrece la posibilidad de ejecutar las instrucciones JavaScript sólo bajo petición. Es decir, si la página web solicitada contiene instrucciones JavaScript, el navegador hará la advertencia oportuna y preguntará si puede ejecutar esas instrucciones. Dependiendo de la página web que usted esté visitando, podrá decidir si el riesgo está justificado o no.



Si se le indica, Internet Explorer puede consultar siempre antes de ejecutar un Java Script.

La idea en sí no está mal, aunque en la práctica resulta muy poco provechosa. Y es que Internet Explorer pregunta, cada vez que hay una página web con instrucciones JavaScript, varias veces para todo el sitio web. Es decir, en cada página nueva efectuará la consulta previamente. Si además se emplean bloques, usted quizá reciba una ventana de aviso por cada uno. De esta manera, acabará con los dedos destrozados de tanto hacer clic antes de que consiga ver algo.

Siempre resulta más práctico dejar que el concepto de zonas de seguridad de Internet Explorer trabaje para usted. Podrá asignar las páginas web para las que quiera autorizar instrucciones JavaScript, a la zona de sitios de confianza donde se permiten scripts. Para todos los demás sitios debería desactivar JavaScript. Desgraciadamente, esto no se puede hacer en Netscape Navigator, que sólo acepta la activación o desactivación completa de JavaScript.

VisualBasic para Internet – VisualBasicScript

Como ocurre siempre que la competencia ha desarrollado una tecnología de éxito, Microsoft tiene que replicar con un desarrollo propio. Para tratar de replicar al competidor Netscape y su JavaScript, los programadores concibieron en Redmond *VisualBasicScript*, abreviado *VBScript*. La idea era aprovechar el lenguaje de programación *Visual Basic*, que en sus distintas versiones tiene que mantener el tipo para muchas cosas, desde la creación de aplicaciones complejas hasta la programación de macros en Office y ahora, también, para programar efectos dinámicos en páginas web. De modo similar a JavaScript, VBScript también es ejecutado por un intérprete especial en el navegador web. Éste restringe las posibilidades de acceso, de modo que no se pueda entrar directamente al sistema de archivos, por poner un ejemplo. Pero como le ocurre a ActiveX, a VBScript tampoco parece aguardarle un gran futuro. Tras haberse hecho fuerte JavaScript a nivel general, Microsoft desechó su proyecto.

INFO

VBScript y esos queridos parientes

En realidad, VBScript es una tecnología bastante segura, ya que el intérprete restringe las posibilidades de aplicar los scripts y, por ejemplo, no permite

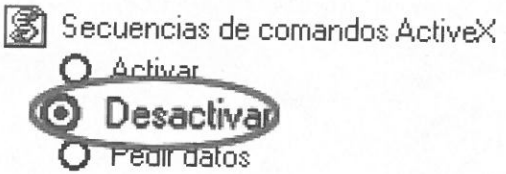
accesos a archivos. Todo podría ser tan idílico y seguro si VBScript no perteneciera a la gran familia VisualBasic. Precisamente este parentesco – en el fondo una ventaja, ya que un programador de VisualBasic puede programar con toda facilidad en VBScript – es lo que convierte a VBScript en un riesgo de seguridad de máximo potencial.

Supongamos la siguiente situación: un VBScript aparentemente inofensivo que produce una pequeña y bonita animación en la pantalla, en segundo plano es mucho más activo. Busca un Winword o Word existente en el PC del usuario y lo arranca. Puesto que Word como lenguaje de macro también habla VisualBasic, VBScript puede direccionar el procesador de textos sin problemas. Abre el archivo *C:\AUTOEXEC.BAT* en el editor y al final le añade la línea *FORMAT C:*. A continuación, guarda el archivo y cierra Word. El usuario ni siquiera se dará cuenta, porque está distraído con la animación. Cuando arranque el PC la próxima vez, llegará la catástrofe y, desgraciadamente, no se trata simplemente de una escena de terror gratuita. Es factible sin más. Por todo esto: ¿VBScript? ¡No, gracias!

Desactivar VBScript

Internet Explorer de Microsoft es el único navegador web que soporta VBScript. Pero también él dispone de una posibilidad para impedir la ejecución de instrucciones script:

1. Desde *Herramientas/Opciones de Internet...* abra las configuraciones de seguridad de Internet Explorer y una vez allí, cambie a la categoría *Seguridad*.
2. Elija la zona de seguridad para la que quiera impedir la ejecución de scripts y después, haga clic sobre el botón *Personalizar nivel...*
3. Busque en la lista la categoría *Automatización*.
4. Desactive la opción *Secuencias de comandos ActiveX*, para impedir la ejecución de las instrucciones VBScript.



Esta opción es suficiente para impedir la ejecución de instrucciones VBScript.

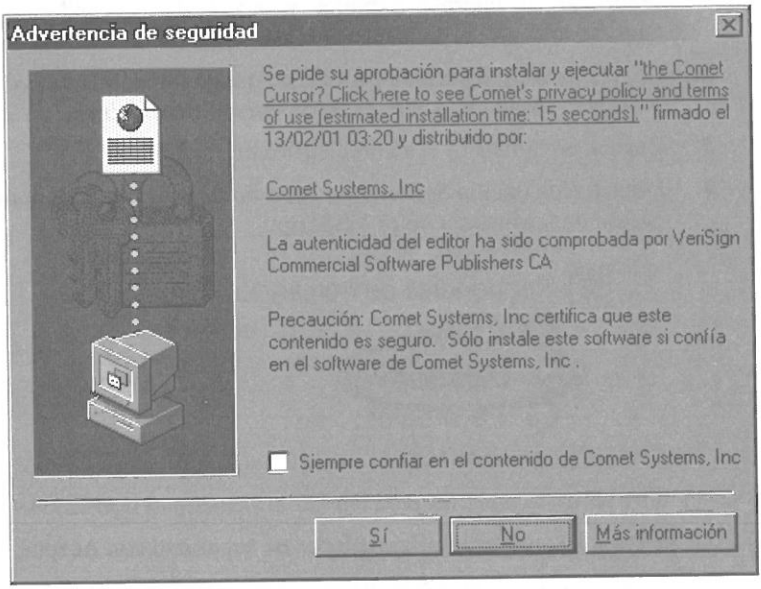
5. Guarde las nuevas configuraciones de seguridad con Aceptar.

Otros navegadores no soportan VBScript de origen, por lo que no es necesario desactivarlo.

Medidas de prevención con los Plug-Ins

Los Plug-Ins son programas adicionales que complementan al navegador web con determinadas capacidades. Éstas casi siempre son la representación de formatos multimedia como archivos de imágenes, sonidos o vídeo. Pero también hay Plug-Ins que presentan en un navegador web archivos de proceso de textos o documentos similares de Office, facilitando al usuario en algunos casos hasta posibilidades limitadas de trabajar con ellos. Desde el punto de vista técnico, los Plug-Ins son programas completamente independientes, que no están sometidos a ningún tipo de restricciones ni vigilancia por parte del navegador web. Los programas adicionales tienen libre acceso al PC y a todos sus recursos. Por lo que, en principio, deberían ser considerados como muy inseguros.

El único factor de seguridad que tienen los Plug-Ins es el buen nombre del fabricante. Frecuentemente, son productores de software renombrados que no se pueden permitir la distribución de programas defectuosos. El origen de un Plug-In se puede comprobar generalmente al bajarlo e instalarlo. Es entonces cuando el navegador web presenta el certificado del Plug-In, donde figura la fuente. Si ésta es de un fabricante de software conocido y su autenticidad queda confirmada, podremos instalar y utilizar ese componente con relativa tranquilidad. Aunque esto tampoco ofrece una seguridad total. Igual que el propio navegador, los Plug-Ins (todavía) pueden incluir agujeros de seguridad desconocidos.



A la hora de instalar Plug-Ins, habría que tener en cuenta la advertencia de seguridad que viene con el certificado del fabricante.

En contraste con los Java-Applets y los componentes ActiveX, los Plug-Ins no pueden llegar a su ordenador sin ser llamados primero. Antes de poder utilizar un Plug-In, deberá bajarlo expresamente de la página web del fabricante e instalarlo. Así, usted es quien controla qué Plug-Ins se ejecutan en su ordenador y cuáles no.

A la hora de bajarse e instalar Plug-Ins, tenga en cuenta las siguientes reglas:

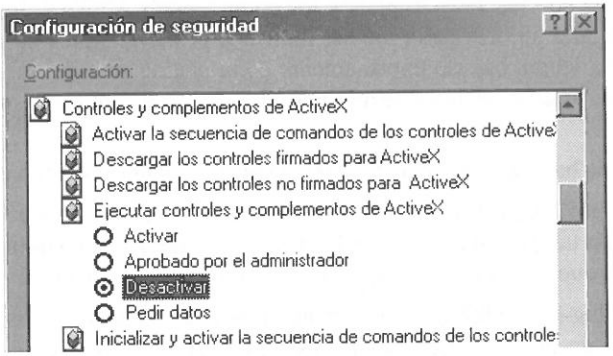
- A ser posible, utilice sólo Plug-Ins de fabricantes de software renombrados. Desista también de recurrir a las versiones nuevas, "recién horneadas". Es mejor que recurra a los Plug-Ins ya establecidos y probados.
- Los Plug-Ins de fabricantes desconocidos sólo los debería instalar, si es que lo hace, por recomendación (un amigo o una revista especializada). Infórmese antes con exactitud sobre la finalidad de ese Plug-In.
- De los Plug-Ins con los que se tope casualmente al navegar por Internet, debería alejarse. Si una página web ofrece maravillosas imágenes o películas que sólo puedan ser vistas con un Plug-In muy concreto; o bien los proveedores quieren ganar dinero con él, o pretenden distribuirlo por algún motivo turbio.
- Instale únicamente los Plug-Ins que realmente necesite. Estos programas no sólo suponen un riesgo de seguridad, casi siempre suelen despilfarrar lo suyo en espacio de memoria.

Podrá obtener información actualizada sobre Plug-Ins en Internet en la dirección http://browserwatch.internet.com/plug-in.html.

Evitar la ejecución de Plug-Ins

Una protección total contra los Plug-Ins destructivos sólo se consigue impidiendo su ejecución para determinadas zonas de seguridad o para todas:

1. Abra desde *Herramientas/Opciones de Internet...* la categoría *Seguridad* donde vienen las configuraciones de seguridad de Internet Explorer.
2. Elija la zona de seguridad para la que quiera impedir la ejecución de Plug-Ins.
3. En ninguno de los niveles de seguridad predefinidos se desactiva totalmente la ejecución de Plug-Ins. Por eso, no importa el nivel de seguridad existente que elija como base. Pero lo mejor es que deje la configuración estándar. A continuación, haga clic sobre el botón *Personalizar nivel...* .
4. Busque en la lista la categoría *Controles y complementos de ActiveX* y marque la opción *Desactivar*, encuadrada en la subcategoría *Ejecutar controles y complementos de ActiveX*.



Así se desactiva en Internet Explorer la ejecución de Plug-Ins.

5. Guarde las nuevas configuraciones con *Aceptar*.

Con esto queda bloqueada la ejecución de todo tipo de Plug-Ins. Si una página web contiene datos Plug-In, Internet Explorer le advertirá mediante una ventana de aviso. Esto es importante, ya que una página web sin los componentes integrados no puede ofrecer el aspecto que diseñó su autor, y los datos Plug-In no pueden ser reproducidos.

TRUCO

Eliminar Plug-Ins

Una vez se tiene un Plug-In en el ordenador, es difícil impedir que se ejecute. Por ello, el método más seguro es desinstalar los Plug-Ins innecesarios. La mayoría de Plug-Ins incorpora un programa de desinstalación. ¿Por qué no comprueba en *Inicio/Configuración/Panel de control* bajo el apartado *Agregar o quitar programas*, si encuentra una entrada que corresponda a un determinado Plug-In? Si no la hay, deberá buscar el directorio de su Plug-In en el disco duro y borrar los archivos manualmente.

3.4 Virus y troyanos – protección contra infecciones digitales

Una de las mayores fuentes de peligro para el PC y sus datos siguen siendo los virus informáticos y sus parientes más cercanos, los caballos de Troya o troyanos. De un modo similar a sus modelos naturales, estos pequeños programas se propagan por sí mismos y se extienden a lo largo de redes y soportes de datos intercambiables, como son los disquetes o CD-ROMs. Con Internet, el peligro que suponen estos viles intrusos aún se ve incrementado en mayor medida. Hoy en día, la interconexión en redes a lo largo de todo el mundo permite que un nuevo virus o troyano se propague en cuestión de pocas horas por todo el globo terráqueo. Por esta razón, siempre que usemos el propio PC para intercambiar datos con otros ordenadores, ya sea mediante soporte de datos, red o Internet, habría que plantearse una protección eficaz contra infecciones.

INFO

Así funcionan los virus

Los virus, en principio, son pequeños programas independientes que ejecutan dos tareas concretas. Una de ellas es la propagación en sí. Todo virus intenta extenderse lo antes posible por muchos otros archivos. Como es activado de nuevo cada vez que se abre un archivo infectado, aún puede seguir propagándose más y más. Esto produce el efecto "bola de nieve", que puede minar un sistema en un tiempo mínimo. Si un ordenador no tiene ningún contacto con el mundo exterior, la infección quedará limitada a él mismo, pero si tiene lugar un intercambio de datos con otros sistemas, bastará un único archivo infectado para que el virus se propague a otros ordenadores. Resulta evidente, entonces, que los virus informáticos puedan propagarse a velocidad de vértigo en un entorno de redes a escala mundial, como Internet. La segunda tarea de los virus suele ser el propio daño que causan. Éste depende totalmente de la imaginación de su programador. Los inofensivos sólo emitirán un mensaje o causarán el colapso del ordenador. Los verdaderos malhechores dañarán archivos y soportes de datos, en algunos casos para siempre.

Protección eficaz contra los virus

Aunque los virus informáticos supongan, sin lugar a dudas, un peligro, quizá alguien podría preguntarse aquí qué tiene que ver este tema con un informe antihacker. En realidad, los virus no son un arma de ataque clásica porque, una vez soltadas las amarras virtuales, ya no se dejan controlar. Pero de hecho, los virus pueden ser empleados con gran eficacia si no se busca selectivamente determinada información, sino que tan sólo se pretende causar daños a una víctima. Estos daños originados por virus informáticos pueden ser cuantiosos, si se emplean virus que destruyan para siempre datos o soportes de datos concretos. Si, por ejemplo, se quiere atacar a una empresa, bastará con filtrar un virus dentro de cualquier ordenador que esté integrado en la red interna de esa empresa. Los vínculos de red son unas rutas de invasión óptimas, a través de las cuales el parásito puede propagarse en muy poco tiempo por la mayor parte de los ordenadores conectados.

INFO

Daños multimillonarios causados por virus

Especialmente en las redes de empresas, los virus informáticos causan cada año daños multimillonarios a escala mundial. Así, empresas de todo el mundo se vieron obligadas a invertir en 1999 un total de 12 mil millones de dólares en la eliminación de virus y de los daños causados por ellos: destrucción de datos y pérdidas de producción resultantes. Pero los especialistas en seguridad suponen que esta siniestra cifra aún es mayor. Muchas empresas no se atreven a reconocer que han tenido problemas con virus, para no preocupar a sus socios y clientes.

(Fuente: http://www.tecchannel.de/news/20000118/thema20000118-508.html)

Para hacer frente a los virus existen, igual que en la vida real, dos posibilidades básicamente diferentes:

- Una buena prevención le protegerá de infecciones de estos pequeños malhechores.
- Si a pesar de todo ocurre el fatídico hecho, ahora habrá que delimitar las consecuencias de la infección y limpiar al ordenador cuanto antes.

En el siguiente apartado vamos a presentarle ambas técnicas, además de consejos para lograr una protección óptima.

Profilaxis – evitar la infección de un virus

La mejor medida contra los virus es no infectarse. A primera vista, esto parece más fácil de decir que de hacer. Pero en realidad, basta con seguir algunas reglas que minimizan el peligro para el propio PC. En principio, un virus sólo puede llegar a su sistema tras el intercambio de datos con otros ordenadores. Es decir, en la vida de todo PC hay ciertos momentos críticos en los que existe peligro potencial. Acostúmbrese a reconocer estas fuentes de peligro:

- Usted mismo puede introducir virus en su sistema cuando inserte *soportes de datos* intercambiables como disquetes, CD-ROMs o discos ZIP.
- Si su PC va vinculado a otros ordenadores a través de redes como puede ser Internet, el peligro puede surgir de varios flancos. Al descargarse software, usted mismo puede infectar a su ordenador. Pero otros también pueden aprovechar los vínculos de red para colocar programas en su PC.
- Si su PC está durante un tiempo sin vigilancia y al alcance de otras personas, puede ocurrir que alguien haga uso ilícito de él sin que usted lo sepa. Esto puede ocurrir con mala intención o incluso por descuido, si por ejemplo un compañero de trabajo le pide a usted "prestado" el ordenador, porque el suyo está siendo reparado.

Medidas de prevención en los soportes de datos

Antes de emplear un soporte de datos, sería recomendable que se planteara si la fuente de los datos es digna de confianza. Si el disquete o CD-ROM procede de un buen amigo, del que sepa que está al corriente sobre los virus y toma las medidas de protección pertinentes, podrá estar más o menos tranquilo. La cosa cambia con los disquetes o CD-ROMs de procedencia dudosa. Si por ejemplo, un conocido le da un disquete diciendo "Mira, me lo ha dado un colega. Tiene un salvapantallas fantástico!", más vale que tenga cuidado.

TRUCO

Jaque mate a los virus de arranque

Las infecciones por virus de arranque se producen muchas veces por una casualidad tonta. Normalmente, un disquete infectado con un virus de arranque no causaría daños si sólo se copian de él archivos. Pero es muy fácil dejar olvidado en su unidad el último disquete que se había empleado. Si sigue ahí la siguiente vez que se arranque el ordenador, éste arrancará desde el disquete en lugar de hacerlo desde el disco duro. Ya tenemos el desaguisado. El virus de arranque ha saltado desde el disquete a su disco duro. Para evitar estos problemas, usted puede dar instrucciones al ordenador para que arranque desde el disco duro, aunque haya un disquete insertado. Este ajuste lo puede hacer en la BIOS de su PC. Allí encontrará en las opciones estándar la secuencia de arranque, donde deberá poner *C:* delante de *A:*. Así, el ordenador siempre leerá los archivos de arranque desde el disco duro, incluso en el caso de que haya un disquete dentro de su unidad. Si por alguna razón se viera obligado a arrancar desde un disquete, tendrá que volver a invertir la secuencia de arranque. Pero en ese caso, asegúrese antes de que el disquete esté limpio de virus.

- Nada más insertar un soporte de datos removible, sométalo a un escáner antivirus. Si éste detecta algo extraño, no pierda mucho tiempo con acciones de limpieza. Saque el soporte de datos de su ordenador y destrúyalo. En el siguiente apartado, le explicaremos cómo emplear correctamente el escáner antivirus.

- Aunque el soporte de datos parezca estar limpio de virus, aún puede haber peligro. A fin de cuentas, podría contener un virus muy reciente que su antivirus aún no conozca. Y aunque sea verdad que el programa no contiene virus, aún puede causar daños. ¿Quién dice que el salvapantallas sólo despliega hermosas imágenes en el monitor? Quizá al mismo tiempo esté borrando datos importantes de su disco duro. Por ello, es recomendable que pruebe sus programas nuevos primero en un entorno de prueba, ya sea un segundo ordenador o un sandbox virtual. Al final de este capítulo, podrá obtener más información sobre cómo probar aplicaciones desconocidas en un entorno seguro.

- Un entorno independiente para probar programas nuevos es un lujo que no está al alcance de cualquiera. Si usted sólo dispone de un ordenador, no tendrá más remedio que probar su nuevo software en él. Pero en ese caso, haga antes sin falta una copia completa de seguridad de su ordenador. Así, si todo falla podrá restaurar siempre el estado original y evitar la pérdida de datos. Para poder probar los nuevos programas con seguridad, una buena alternativa sería un segundo sistema operativo instalado en paralelo.

Medidas de prevención en las redes

Para los PCs integrados en entornos de red, en principio rigen las mismas reglas que para el intercambio de información con soportes de datos removibles. Si usted carga software procedente de la Red, lo mejor será que lo trate como si procediera de un disquete. Pero la Red emana un peligro adicional, procedente de los otros ordenadores integrados o de sus usuarios. Mientras exista un vínculo físico entre su PC y otros, cualquiera podrá abusar de éstos para transferir datos a su ordenador, por ejemplo, troyanos. Si quiere reducir este peligro, no debería mantener en marcha esos vínculos de red más tiempo que el estrictamente necesario. En las conexiones de acceso telefónico a través de módem, la mayoría de los usuarios ya están pendientes del tiempo, aunque sólo sea pensando en la factura del teléfono. Pero si usted dispone de tarifa plana o está en la red de su empresa, tampoco hace falta que se mantenga todo el día conectado. Si por ejemplo necesita acceder al servidor de archivos o de impresora de su red con muy poca frecuencia, es mejor que sólo se conecte como usuario.

Ejecute regularmente tests de antivirus en su ordenador y anime a los demás usuarios a hacer lo mismo. La experiencia ha demostrado que en una red de ordenadores donde no se toman medidas de protección contra los virus, basta con una infección localizada en un solo punto para que en un breve espacio de tiempo, toda la red acabe contaminada. Los actuales programas antivirus ofrecen la posibilidad de ejecutar, a intervalos ajustables según las necesidades, scans completos de todos los soportes de datos conectados.

Medidas de prevención contra el uso ilícito

Mientras usted esté sentado ante su PC, podrá tener bajo control la mayor parte de los puntos críticos. ¿Pero qué ocurrirá si deja su ordenador sin vigilancia y lo utiliza otra persona? También un compañero de trabajo que, en su ausencia, "tome prestado" un ratito el ordenador porque quizá no posea uno propio, podría contraer un virus. Sólo que en este caso, usted no sabría nada y el virus quizá tardara algún tiempo en ser detectado, con lo que podría completar su obra destructiva con toda tranquilidad. Para protegerse de este peligro, restrinja el acceso a su ordenador totalmente para todos los que no tengan permiso. Aunque precisamente en los PCs esto resulta difícil, ya que en caso de duda se dejan arrancar desde disquete. Pero esto se puede evitar haciendo las correspondientes configuraciones en el BIOS de su ordenador. En el Capítulo 2 hay instrucciones detalladas sobre cómo restringir el acceso a su ordenador.

TRUCO

Proteger la unidad de disquetes

Para proteger eficazmente las unidades de disquetes durante su ausencia, hay candados de disquetes. Estos dispositivos mecánicos se insertan en la disquetera como si fueran un disquete y se cierran con una llave. Esto blo-

quea la unidad para cualquier disquete. El candado sólo puede ser retirado con su llave. Estos aparatos pueden adquirirse en comercios especializados. Para las unidades de CD y DVD, que pueden ser abiertas electrónicamente pulsando un botón o haciendo clic con el mouse, hay soluciones de software comparables que bloquean la apertura de la unidad mediante contraseña.

Escáner antivirus – ¿Doy positivo?

Por muchas medidas de prevención que aplique, usted jamás debería renunciar al empleo de un escáner antivirus actualizado. Éste minimizará los últimos riesgos e intervendrá en caso de emergencia, si a pesar de todo usted olvidó o ignoró alguna medida de prevención. Hoy en día, la mayoría de PCs ya se suministran con un software antivirus. Si aún no hubiera instalado ninguno, a continuación le detallamos el procedimiento básico con el ejemplo de *AntiVir*, un escáner antivirus gratuito para el uso de particulares y que podrá descargar bajo la dirección http://www.hbedv.com

TRUCO

Compruebe su antivirus

Si usted no ha encontrado nunca ningún virus en su PC, ¿cómo puede estar seguro de que su programa antivirus funciona correctamente? Emplear un virus auténtico, quizá sea demasiado arriesgado. Además, en la mayoría de los casos no se tiene ninguno a mano. Pero existe un sencillo test desarrollado por el *European Institute for Computer Anti-Virus Research* (EICAR). Para utilizarlo, sólo necesitará crear un archivo de texto sencillo (texto ASCII, ¡no un documento de proceso de textos!) en su ordenador y escribir en él la siguiente cadena de caracteres:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

(Importante: ¡todas las letras están en mayúsculas y el tercer carácter es la letra O, no el dígito 0!)

Esta combinación de caracteres es una firma de virus que todo programa antivirus debería advertir cuando usted someta al archivo a un test. Naturalmente, este "virus" no supone un peligro real porque se replica sólo o causa cualquier otro daño. Aun así, permite comprobar la eficacia de sus medidas preventivas. Podrá obtener más información sobre el virus de prueba EICAR bajo la dirección:

http://www.eicar.org/anti_virus_test_file.htm.

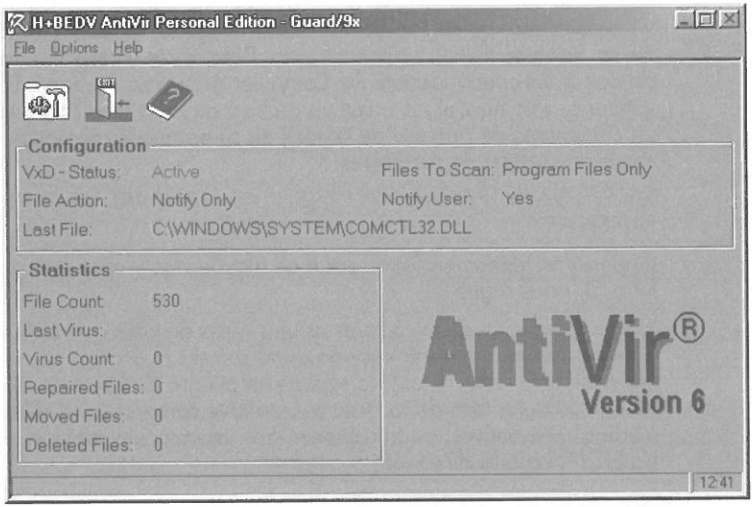
Escáner de virus en segundo plano

La solución más fiable y segura para detectar un virus es emplear un escáner de segundo plano permanente. Se trata de un módulo de programa que en cada arranque del ordenador, es cargado en una memoria de trabajo donde permane-

cerá. Controlará en segundo plano todos los accesos a archivos y explorará todos los archivos abiertos, almacenados y de nueva creación, para ver si contienen virus. Esta solución resulta tan fiable porque examina inmediatamente todos los archivos recién importados o que estén siendo creados. Por eso, un nuevo virus ni siquiera tiene oportunidad de propagarse, ya que es detectado y eliminado inmediatamente. Al instalar AntiVir, se activa automáticamente un escáner en segundo plano llamado *Guard*. Se puede comprobar que está activado por el símbolo rojo que aparece en la parte inferior derecha en la barra de inicio. Aunque debería comprobar sin falta las configuraciones del módulo Guard y adaptarlas, si fuera necesario.

El símbolo dentro de la barra de inicio muestra la actividad del módulo Guard.

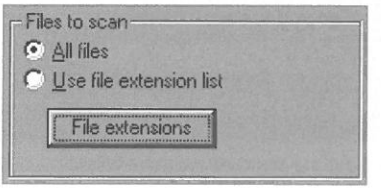
1. Para cambiar las configuraciones del módulo Guard, haga doble clic sobre el símbolo de AntiVir Guard en la barra de inicio. Con esto abrirá el programa de control de Guard, que le dará en primer lugar una visión de conjunto sobre las configuraciones actuales de ese componente.



En el programa de control para el módulo Guard es donde se ajustan las configuraciones.

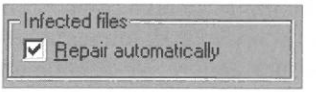
2. Con la opción de menú *Options/Options* abrirá el menú de configuración en sí, que está subdividido en varias categorías. En la categoría *Scanner* (búsqueda), encontrará en primer lugar las configuraciones generales para el comportamiento de AntiVir-Guard.

3. En el área *Files to scan* (archivos a comprobar), usted decide en primer lugar si el escáner de segundo plano debe explorar todos los archivos (*All files*) o sólo archivos que tengan una extensión determinada (*Use file extension list*). Esta última es la configuración estándar, aunque sólo buscará virus en los archivos ejecutables, por lo que el escáner pasaría por alto los virus de macro ocultos en documentos de Office. Por eso, le recomendamos la exploración de *Todos los archivos*.



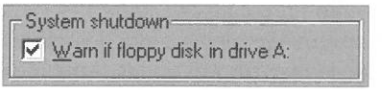
Por precaución, solicite la exploración de todo tipo de archivos.

4. En el apartado *Infected files* (archivos infectados), usted puede decidir si el módulo Guard debe intentar la limpieza y reparación de los archivos infectados automáticamente. Esto último es algo que no resulta factible con todos los virus. Aun así, es aconsejable marcar la opción *Repair automatically* (reparar automáticamente).



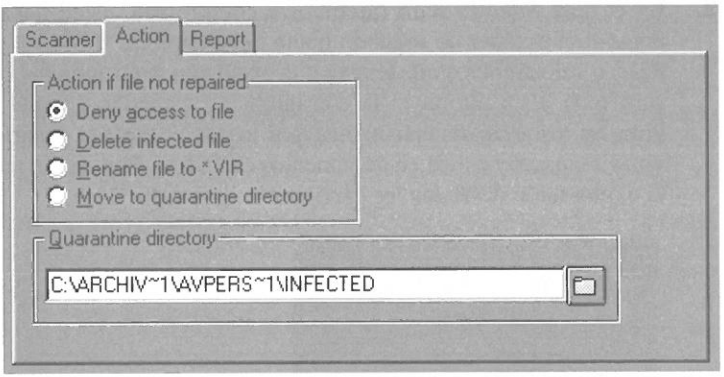
Solicite la limpieza y reparación de los archivos infectados.

5. Finalmente, bajo *System shutdown* encontrará una función que de vez en cuando puede ser útil. Si activa la opción *Warn if floppy disk in drive A:* (avisar si hay un disquete en la unidad A:), cuando apague el sistema, Guard le avisará si queda algún disquete en la unidad. Esto le protegerá de que ese disquete sea inicializado accidentalmente la próxima vez que usted arranque el ordenador. Si bien también puede evitar que usted olvide un disquete con datos confidenciales dentro del ordenador.



Los disquetes olvidados dentro de la unidad son una fuente de peligro.

6. Cambie después a la categoría *Action* (acción) para decidir qué hacer con un archivo infectado que no pueda ser reparado automáticamente, o en caso de que la función de reparación no esté activada. Aquí puede elegir entre varias posibilidades:



Elija el destino de los archivos que no puedan ser reparados.

7. En el área *Action if file not repaired* (acción a desplegar si el archivo no puede ser reparado) encontrará cuatro opciones. Éstas representan soluciones cuya seguridad es menor, conforme se va bajando en la lista. *Delete infected file* (borrar archivo infectado) es la variante más radical y segura. También es relativamente segura la opción *Move to quarantine directory* (mover a directorio de cuarentena), que desplaza al archivo al *Quarantine directory* (directorio de cuarentena) indicado en el campo de la parte inferior. En *Rename file to *.VIR* (renombrar archivo como *.VIR), el archivo problemático sólo recibirá un sufijo nuevo que, al menos, evitará en gran parte su posterior ejecución o apertura. *Ignore file* (ignorar archivo) es una solución poco recomendable, ya que el archivo es conservado tal cual.

8. Guarde las nuevas configuraciones con OK o Aceptar y cierre el programa de control con *File/Exit and minimize* para finalizar el programa de control, aunque dejando que el módulo Guard siga trabajando en segundo plano.

Antivirus manuales

Como complemento a un escáner de segundo plano permanentemente activo, se puede ejecutar en cualquier momento un escáner de antivirus manual. Al hacerlo, el software antivirus analiza sistemáticamente todos los archivos existentes para detectar infecciones. Esto puede resultar útil en las siguientes situaciones:

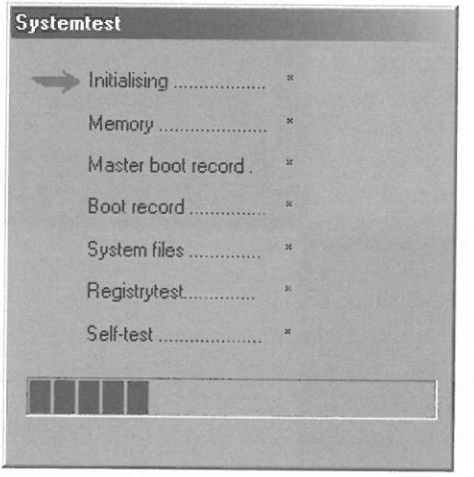
- Antes de activar por primera vez un escáner de segundo plano, sería recomendable ejecutar al menos un scan manual para asegurarse de que en ese momento, el PC se encuentra "limpio". Sólo así podrá confiar en que el escáner de segundo plano proporcione realmente una protección fiable a su ordenador.

- Si en algún momento el escáner de segundo plano ha estado inactivo, se debería realizar posteriormente un scan manual para verificar si el PC está en condiciones seguras. La desactivación del scan en segundo plano pudo ser causada, si por ejemplo al arrancar el ordenador en modo protegido, el antivirus sufre un fallo total causado por un defecto del sistema, o si fue desconectado por alguna razón.
- Si el PC fue utilizado durante una ausencia por otro usuario y no tenemos la seguridad de si éste pudo desconectar temporalmente el antivirus de segundo plano.

Finalmente, el scan manual también puede ser una alternativa general al escáner de segundo plano. Si usted por ejemplo realiza pocos intercambios de datos con otros PCs, podría resultar más práctico renunciar a un escáner de segundo plano que acaba afectando al rendimiento y, en su lugar, ejecutar regularmente scans o búsquedas manuales, aunque éstas no proporcionen un nivel de seguridad tan elevado.

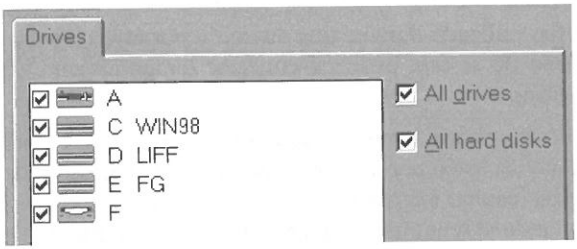
Búsqueda de virus con AntiVir

1. Para ejecutar un scan manual con AntiVir, arranque primero desde *Inicio/Programas/AntiVir 9x Personal Edition/AntiVir 9x* el programa principal de AntiVir. El programa verificará la memoria de trabajo en primer lugar, los sectores de boot y los archivos de sistemas, para ver si presentan huellas de virus que quizá ya estén activos y pudieran manipular los resultados.



Durante al arranque, AntiVir comprueba si ya hay virus activos.

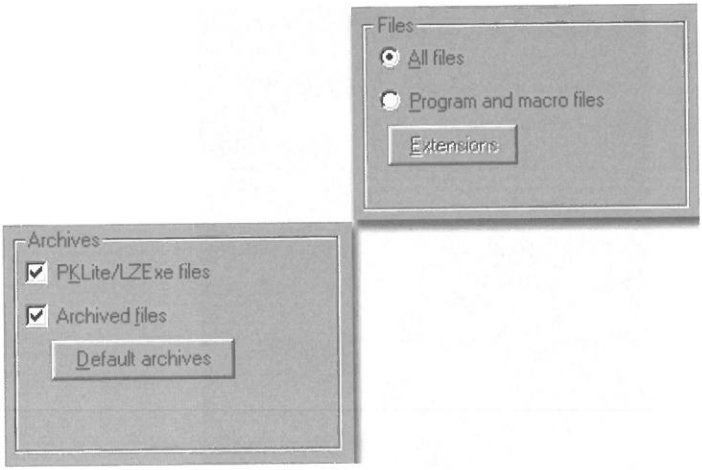
2. A continuación, arranca el verdadero programa principal. Aquí se debería definir primero en el área *Drives* los discos que se necesite verificar. Lo más seguro es hacer un scan completo con la opción *All drives*. Pero también puede elegir unidades concretas para hacer un scan selectivo de los mismos después del intercambio de archivos.



Seleccione los discos que deban ser verificados.

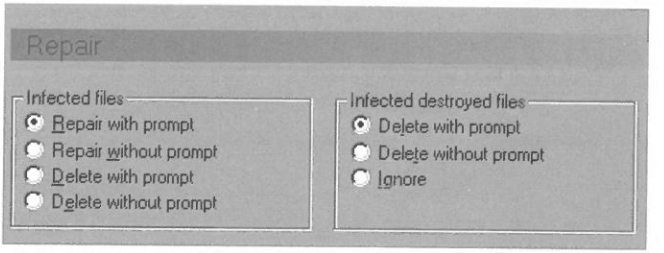
3. Antes de comenzar con el propio scan o verificación, debería comprobar las configuraciones más importantes del programa y, si fuera necesario, ajustarlas. Para eso abra las configuraciones con *Options/Configuration*.

4. Aquí deberá definir primero, en el apartado *Search*, los archivos que deban ser explorados. Active en el área *Files* la opción *All files* (todos los archivos), para escanear realmente todo tipo de archivos. Active también en el área *Archives* la opción *Archived files*, para escanear de igual forma los archivos ZIP o similares, que serán descomprimidos temporalmente por AntiVir y examinados.



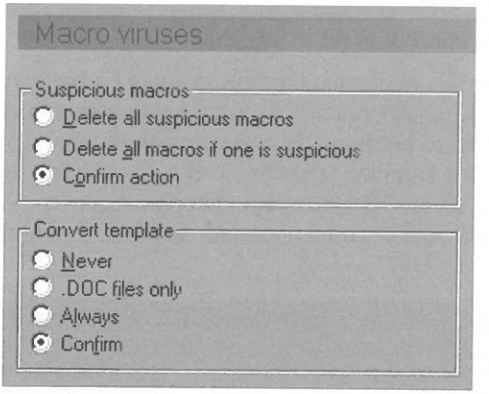
Active la búsqueda para Todos los archivos y para Archivos compactados.

5. Cambie después al apartado *Repair* (reparar) y seleccione las opciones *Repair with prompt* (reparar con consulta) y *Delete with prompt* (borrar con consulta) respectivamente. Con esto activará el modo interactivo, que le advertirá de cada virus que encuentre y le permitirá decidir qué hacer con él. Así, puede mantener un control total sobre el proceso.



Decídase siempre por la acción con consulta para realizar la verificación en modo interactivo.

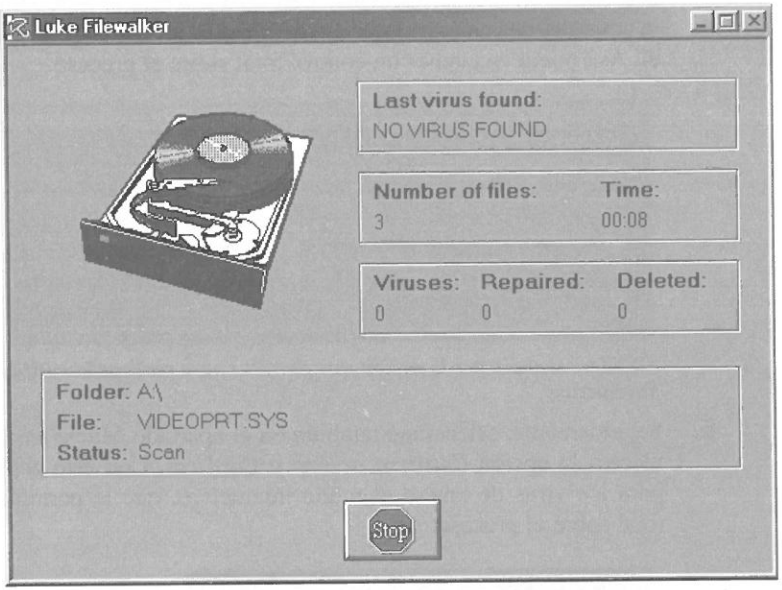
6. Seguidamente, seleccione también en el apartado *Macro viruses* (virus de macro) la opción *Confirm action y Confirm*. Con esto activará también para los virus de macro el modo interactivo, que le permitirá un control total sobre el proceso.



También en los virus de macro debería seleccionar siempre las opciones interactivas con consulta.

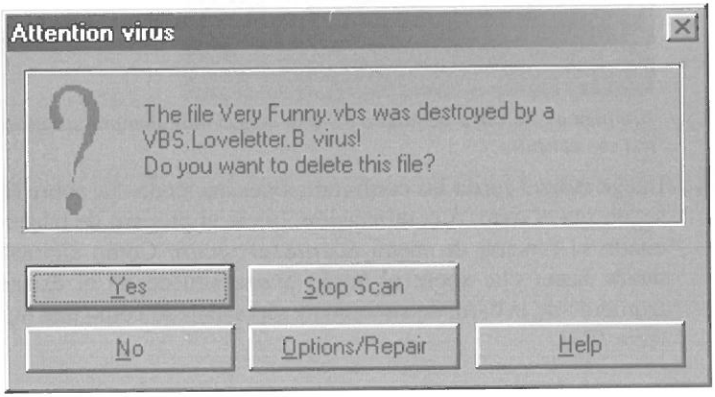
7. Luego deberá cerrar las configuraciones haciendo clic sobre *OK o Aceptar*, según sea el caso. A continuación, inicie el proceso de búsqueda seleccionando la función de menú *Scan/Start scan*. Como alternativa, también puede hacer clic sobre el botón *Scan*, situado en el extremo superior izquierdo de la barra de símbolos y representado como una lupa, o pulsar la tecla *[F2]*.

8. Ahora, AntiVir iniciará la verificación de las unidades indicadas. Podrá seguir el proceso desde una ventana de estado.



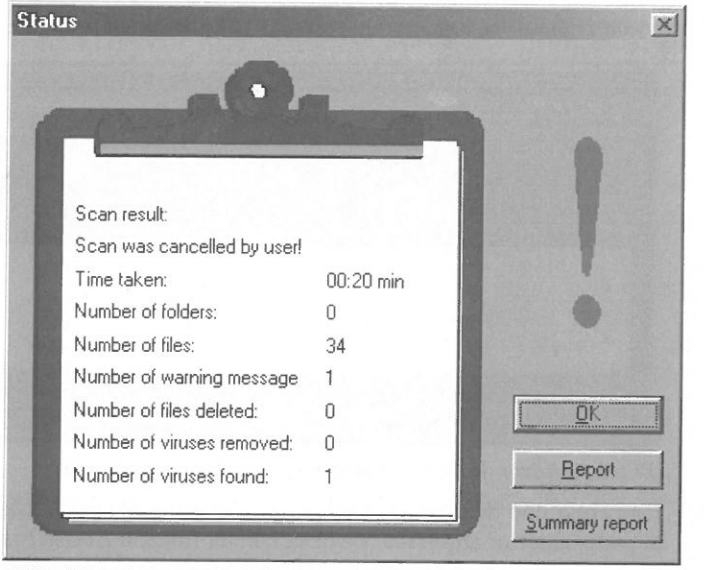
AntiVir verifica los discos de su PC.

9. Si AntiVir descubriera realmente un virus, actuará en función de las configuraciones elegidas anteriormente. Si usted había activado el modo interactivo con consulta, el programa le presentará ahora una ventana de aviso donde podrá ver los archivos afectados y el virus que los infectó. Ahora, podrá decidir si el archivo debe ser reparado o no. Si no es posible la reparación, usted podrá decidir en otra ventana de aviso si el archivo debe ser borrado o ignorado.



AntiVir ha encontrado un archivo infectado ¿Qué hacer ahora?

10. Tanto si AntiVir ha detectado un virus como si no, al finalizar el proceso de búsqueda usted recibirá siempre un resumen. Compruebe en él si todos los virus hallados (suponiendo que se hallara alguno) fueron realmente eliminados. De no ser así, debería tomar más medidas para limpiar o borrar los archivos afectados.



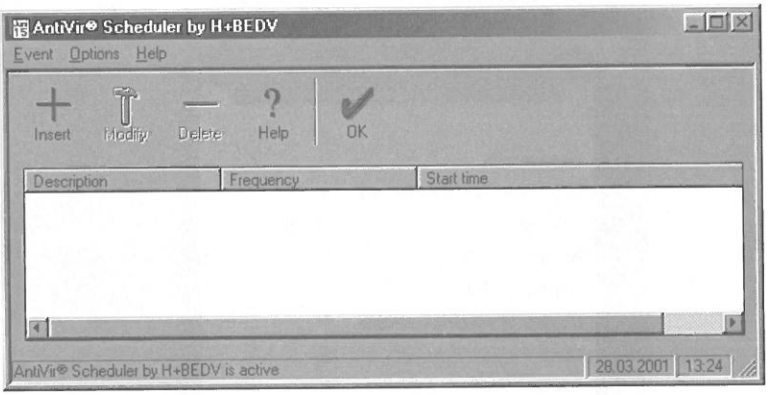
Al finalizar el proceso de búsqueda, obtendrá un resumen de los resultados.

Si durante un proceso de scan o búsqueda se detectaron virus, debería repetir enseguida el scan para asegurarse de que fueron limpiados realmente todos los archivos infectados y que el virus fue erradicado del sistema. Si el scan original fue delimitado a una sola parte de los discos, sería recomendable ampliar sin falta la búsqueda de control a todos los discos. Además, resulta recomendable verificar también los disquetes empleados recientemente. Si usted usa una grabadora de CDs, sería más seguro comprobar también los últimos CDs que grabara con ella.

Antivirus con temporizador

Una alternativa al sistema de segundo plano y a las búsquedas manuales, son las ejecuciones de verificación con tiempo programable. Al igual que casi todos los antivirus modernos, AntiVir también ofrece esa posibilidad. Para ello, dispone de un módulo propio llamado *Scheduler*. Este módulo le permitirá ajustar cuándo o con qué frecuencia AntiVir deberá verificar automáticamente el PC.

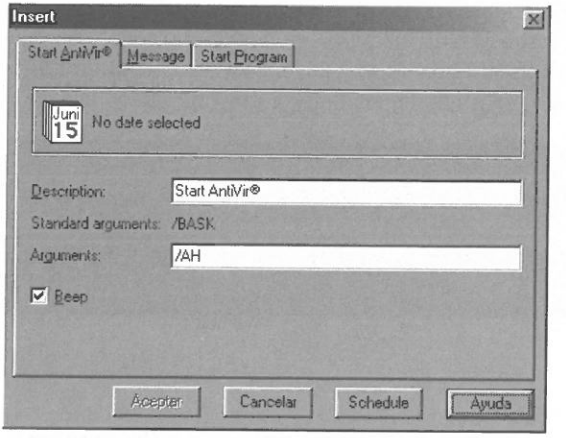
1. Para arrancar el componente de planificación de AntiVir, siga la secuencia de menú *Inicio/Programas/AntiVir 9x Personal Edition/AntiVir Scheduler*. El programa consta de una sencilla ventana, donde se especifican los eventos ante los que AntiVir debe actuar. Naturalmente, esta lista estará vacía al principio. Le corresponderá a usted programar, de modo similar a lo que se hace en un vídeo, los sucesos ante los que deberá reaccionar AntiVir.



El temporizador de AntiVir puede ser programado con eventos.

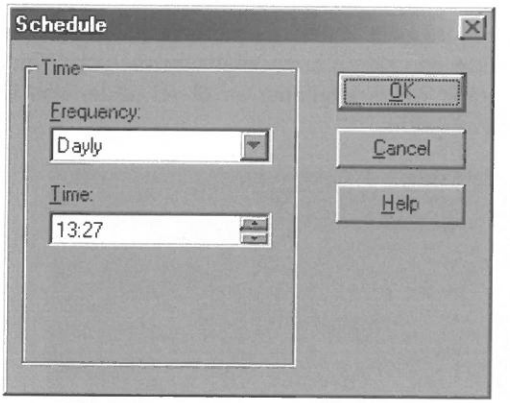
2. Para crear uno de estos sucesos, haga clic sobre el botón *Insert* situado en la parte superior izquierda, o seleccione la función *Event/Insert*. Con esto abrirá el menú de inserción, donde podrá realizar bajo diferentes categorías todas las configuraciones fundamentales.

3. En la categoría *Start Antivir* primero definirá con qué parámetros deberá ejecutarse AntiVir. Por ejemplo, podrá indicar en el campo *Arguments* las letras de los discos que deban ser verificados (*A: C: D:*). Igualmente, podrá definir parámetros especiales de AntiVir. El parámetro */AH* por ejemplo, se encarga de que sean escaneados todas las unidades del disco duro *-/A(ll) H(arddisks)-*. Si usted conserva el argumento estándar */BASK*, AntiVir será arrancado con las configuraciones que usted definiera en el programa principal.



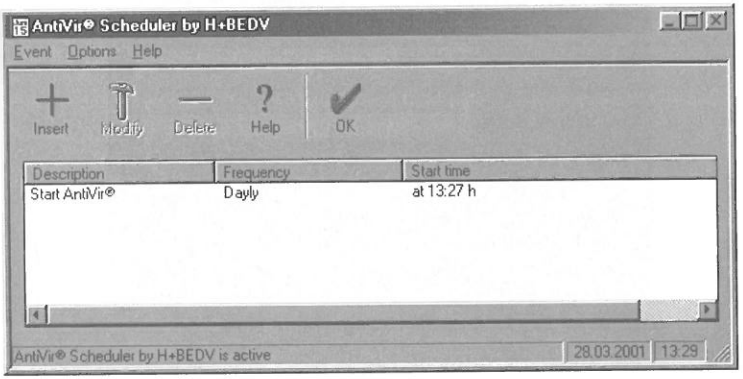
Defina los parámetros de arranque para el escáner automático.

4. A continuación, haga clic en la parte inferior sobre el botón *Schedule*, para definir en la ventana *Schedule* el momento en que tendrá que ser ejecutada la búsqueda. Dentro de esta ventana, elija primero *Frecuency*. Aquí puede hacer que cada evento o suceso de scan sea ejecutado *Single* (Una única vez), *Daily* (Diariamente), sólo los Días laborables (*Workday*), o *Weekly* (Semanalmente). En función de lo que haya elegido, cada selección le proporcionará más posibilidades de configuración. Para la ejecución única o semanal, tendrá que determinar la hora y la fecha o día de la semana. Si la ejecución es diaria o en días laborables, sólo necesitará ajustar una hora. Guarde la planificación haciendo clic sobre *OK*.



Fije el momento de arranque del scan automático.

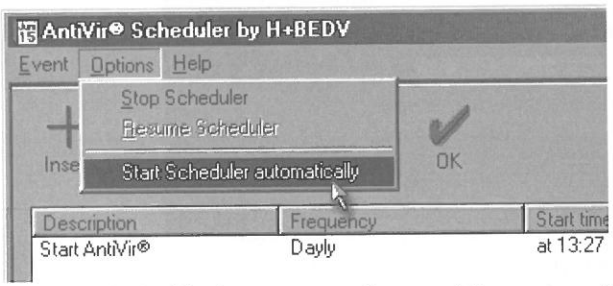
5. De vuelta a la ventana anterior del evento *Insert*, confirme las configuraciones de dicho evento mediante un nuevo clic sobre *OK*. Con esto quedará definitivamente creado el nuevo suceso. Cuando vuelva a la ventana principal del planificador, encontrará una entrada en la lista de eventos.



El evento para un scan antivirus automático ha quedado programado.

De este modo podrá programar más eventos, por ejemplo para controlar con diferente frecuencia discos que estén amenazados por peligros de distinta gravedad. Siempre que llegue el momento programado, el planificador arrancará AntiVir automáticamente y le hará ejecutar el proceso de búsqueda. Para ello, sólo deberán cumplirse dos condiciones:

- El PC deberá estar en marcha en ese momento. Para cumplir esta premisa, lo mejor será que elija fechas en las que su ordenador sea usado normalmente.
- El planificador deberá estar activo. El método más fiable para lograrlo es hacer que sea arrancado siempre automáticamente con Windows. Para tal fin, active la opción correspondiente en el scheduler con *Options/Start Scheduler automatically*.



Haga que el planificador sea arrancado automáticamente con Windows.

Espías en la sombra – los caballos de Troya

Ahora que casi todo el mundo es consciente del peligro que suponen los virus, va apareciendo en las redes una nueva amenaza que frecuentemente supone un peligro aún mayor. Los caballos de Troya – llamados brevemente troyanos – son una modalidad especial de intrusos. La mayoría de las veces no tienen ninguna intención destructora. Lo que pretenden es espiar información confidencial. Por ello, anidan en el ordenador de manera parecida a los virus y espían ocultos en la sombra. Así pueden leer o manipular datos importantes, al igual que registrar las veces que el usuario pulsa las teclas, para averiguar la contraseña.

INFO

¿Qué significa caballo de Troya?

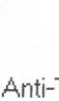
La expresión "Caballo de Troya" tiene su origen en el mito de la lucha por Troya, ciudad de la antigua Grecia que acabó siendo conquistada con una artimaña. Los sitiadores regalaron a los troyanos un gigantesco caballo de madera como "regalo de reconciliación". Los habitantes lo remolcaron hasta el interior de la ciudad y celebraron su supuesta victoria. Pero dentro del caballo de madera se escondían soldados, que salieron al amparo de la oscuridad y abrieron las puertas de la ciudad para dejar entrar a sus camaradas. Entre todos, vencieron fácilmente a los habitantes embriagados tras la fiesta. A esta leyenda se remonta hasta hoy el nombre de una argucia, con la que se puede conseguir acceso ilícito.

Desenmascarar a los caballos de Troya

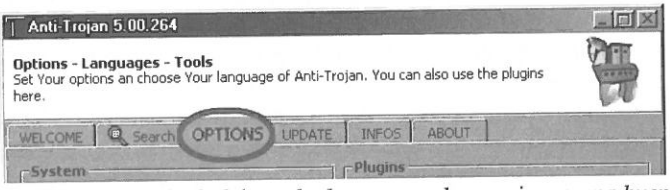
La detección de troyanos puede ser comparada de algún modo con la búsqueda de virus informáticos. Por eso los programas antivirus ya proporcionan cierta protección. Aunque es más seguro emplear un programa especial que se dedique enteramente a combatir estas puertas traseras secretas. Uno de los mejores de este tipo es *Anti-Trojan*, que puede encontrar bajo la dirección http://www.anti-trojan.net como versión de prueba gratuita. Este programa conoce las huellas típicas de más de 5.000 troyanos y no sólo los puede detectar, sino también eliminar de raíz.

1. Anti-Trojan viene como archivo de instalación de descompresión automática, que usted sólo necesitará ejecutar. Una vez instalado correctamente, podrá activar el programa desde *Inicio/Programas/Anti-Trojan/Anti-Trojan 5.0*

2. Tras el arranque, en primer lugar le saludará la ventana de registro. La versión gratuita de prueba de Anti-Trojan se deja arrancar en total cinco veces. A partir de ahí, quien quiera seguir utilizándolo tendrá que registrarse. Confirme esta advertencia haciendo clic sobre el botón *Continue*.

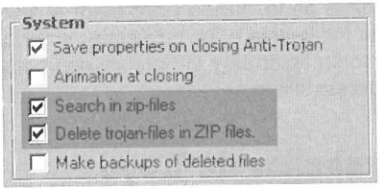


3. A continuación, llegará a la ventana principal de Anti-Trojan que viene subdividida en varias categorías. Cambie primero a la categoría *Options* para controlar las configuraciones básicas.



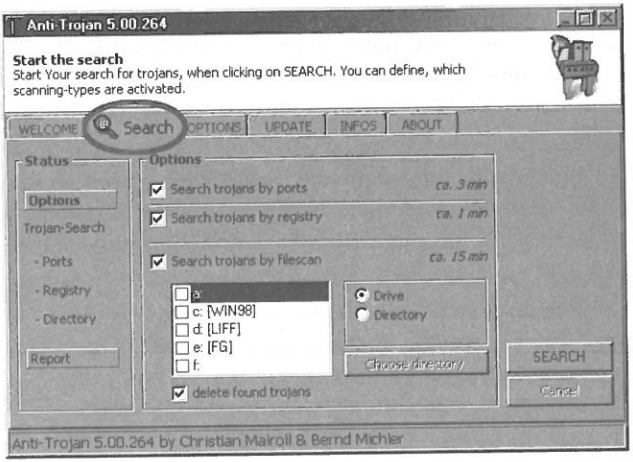
Antes de emprender la búsqueda de troyanos, haga primero una buena configuración de Anti-Trojan.

4. Dentro del área System conecte las opciones *Search in zip-files* (buscar en archivos Zip) y *Delete trojan-files in ZIP files* (eliminar troyanos en archivos Zip), para incluir también los archivos ZIP en la búsqueda de troyanos. Esto ralentiza el proceso de búsqueda, pero es mucho más seguro, ya que a los troyanos les gusta esconderse en archivos ZIP descargados.



Active estas opciones para detectar troyanos también en archivos ZIP.

5. Para comenzar ahora la propia exploración en busca de troyanos, cambie a la categoría *Search* (búsqueda).



Dentro de la categoría Search están las diferentes opciones de búsqueda.

Detectar troyanos mediante portscans o verificador de puertos

Una buena posibilidad para detectar troyanos son los portscans. Para que los espías troyanos puedan transmitir al hacker los datos recopilados, necesitan utilizar el vínculo de red del PC. Un portscan verifica estos vínculos de red para ver si hay datos sospechosos y así poder detectar la actividad de un troyano.

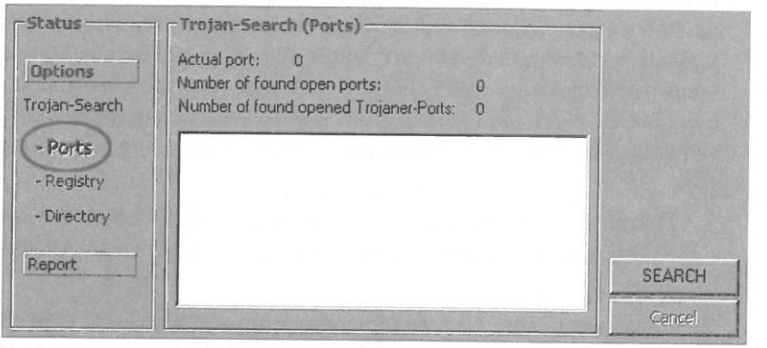
INFO

¿Qué es un puerto?

Para que un PC pueda ser enlazado con una red como puede ser Internet, deberá disponer de un vínculo de red. Éste funciona paralelamente a varios niveles para que distintos servicios puedan ser utilizados al mismo tiempo. Esto se puede comparar con una autopista, que tiene diferentes carriles para que varios coches la puedan recorrer simultáneamente en ambas direcciones. En la red, los distintos carriles se llaman puertos. Hay una serie de puertos estándar (por ejemplo el Puerto 80 para los servidores web). Aparte de éstos, quedan disponibles algunos miles de puertos libres que pueden ser utilizados por los programas que lo necesiten (tanto para lo bueno, como para lo malo).

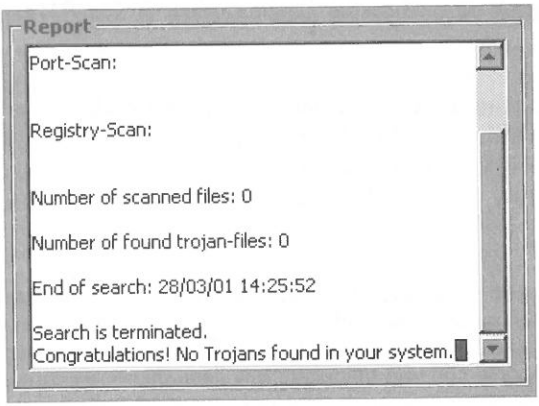
1. Para ejecutar un portscan en su PC, marque la casilla *Search trojan by ports* y seleccione dentro del área *status*, a la izquierda bajo *Trojan-Search*, la función *Ports* (Puertos).

2. A continuación, Anti-Trojan visualizará el menú de portscan, que podrá iniciar haciendo clic sobre el botón *Search* (Buscar), situado en el extremo de la derecha.



Con un portscan, puede buscar transferencias de datos sospechosas desde su PC a Internet.

3. Después, el programa verificará todos los puertos existentes en busca de huellas sospechosas. Usted podrá controlar el progreso desde el campo de estado. Al finalizar, recibirá un informe con los resultados de las búsquedas.



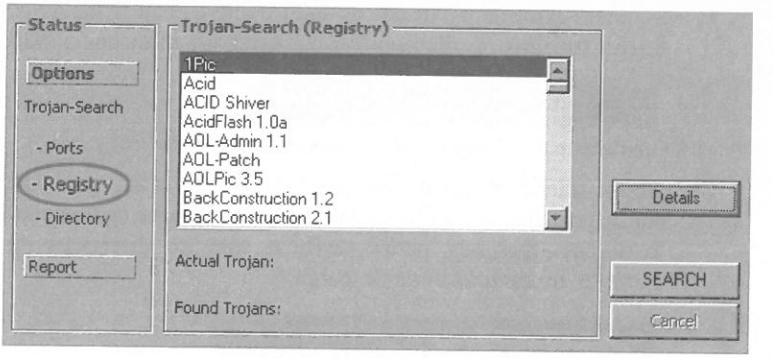
El resultado del portscan lo saca a la luz.

Cuando ejecute un portscan, tenga en cuenta que no todo puerto abierto debe ser atribuido inmediatamente a un troyano. Si usted ha instalado por ejemplo el servidor "Personal Webserver" u otro servidor web, éste utilizará correctamente el Puerto 80. Pero si Anti-Trojan advierte de puertos abiertos donde pueda haber troyanos, usted debería realizar sin falta más pruebas.

Verificar el registro

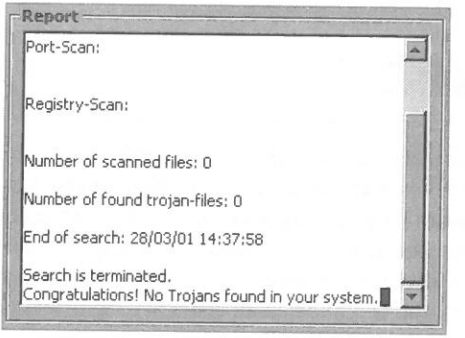
La mayoría de los troyanos dejan huellas en el registro de Windows. El registro es una base de datos donde se almacenan todas las configuraciones del Windows y de las aplicaciones instaladas. Además, en él se establece también qué programas deben ser ejecutados al arrancar el sistema. El registro no tiene protección y puede ser manipulado sin problemas. Esta circunstancia la aprovechan los troyanos para anidar en un PC basado en Windows y recopilar datos. Por ejemplo, efectúan entradas para ser cargados y activados automáticamente cada vez que arranque Windows. Anti-Trojan puede detectar estas huellas y eliminar las entradas.

1. Para que el registro de su PC sea examinado, deberá activar en el menú *Search* la opción *Search trojans by registry* (Buscar troyanos en el registro).
2. A continuación, elija en *Options* la función *Registry*. Con esto abrirá una lista de todos los troyanos conocidos por Anti-Trojan, que dejan huella en los datos del registro.
3. Para arrancar el test, haga clic sobre el botón *Search*.



Con la opción de búsqueda Registry, se escanea el registro de Windows en busca de huellas de troyanos.

4. Ahora, Anti-Trojan recorrerá toda la lista y verificará para cada troyano si sus huellas típicas pueden ser encontradas en el registro. También en este caso, se recibirá un informe completo.



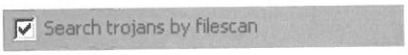
Ha habido suerte: este PC está libre de troyanos.

Si Anti-Trojan hiciera algún hallazgo durante la verificación del registro, podrá eliminar inmediatamente las entradas correspondientes. Así se evita eficazmente que durante el siguiente arranque de Windows, el troyano se vuelva a activar.

Explorar las unidades en busca de troyanos

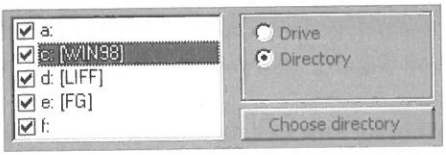
Por último, Anti-Trojan no sólo es capaz de detectar huellas de las actividades de troyanos, sino también del propio malhechor. Para ello, explora los archivos de todos los discos del PC en busca de firmas de troyanos, es decir, estructuras típicas de datos que denoten el código de un programa troyano concreto. Los archivos que pertenezcan a ellos pueden ser borrados de inmediato para erradicar eficazmente a los troyanos.

1. Si quiere explorar los discos de su PC, active en la pestaña *Search* la opción *Search trojans by filescan* (buscar troyanos en discos o unidades).



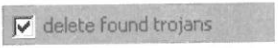
Active esta opción para pedir la exploración de los discos duros.

2. Ahora, seleccione los discos que quiera verificar. A ser posible, en el primer control debería incluir todas las unidades, aunque esto pueda llevar bastante tiempo. Después, podrá verificar sólo los diferentes directorios, por ejemplo, un directorio de descarga.



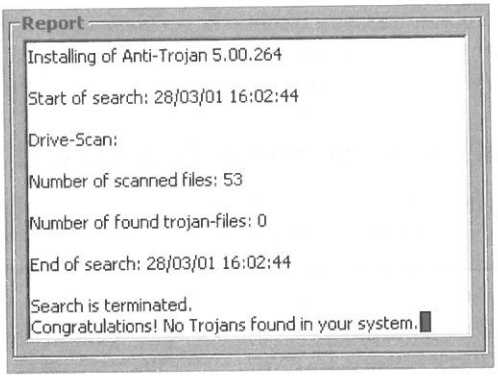
Seleccione los discos y directorios que deban ser explorados.

3. Importante: para que los troyanos detectados sean erradicados inmediatamente, active la opción *Delete found trojans.*



Haga que los troyanos detectados sean erradicados inmediatamente.

4. A continuación, inicie la verificación con *Search*. Anti-Trojan verificará ahora todos los archivos que estén en las unidades indicadas, descomprimiendo temporalmente hasta archivos compactados y chequeándolos, para que nada sea pasado por alto. A continuación, usted recibirá de nuevo un informe final. Si lo cierra y le aparece el mensaje *No trojans found in your system* (no se detectaron troyanos en su sistema), significará que todo está en orden.

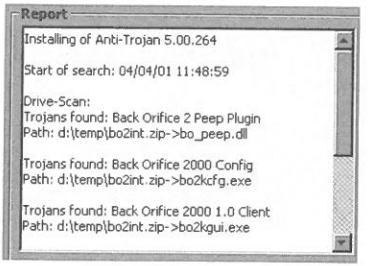


No se han detectado huellas de troyanos.

¿Se han encontrado troyanos?

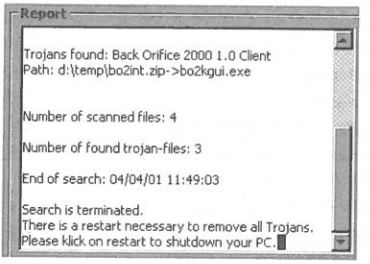
Sin embargo, hay que temer que de vez en cuando Anti-Trojan sí se tope con algún troyano. Pero esto es bueno. Significa que al menos, usted ha detectado al troyano y podrá hacer que Anti-Trojan lo erradique enseguida.

1. Si antes de empezar la verificación conectó la opción *Delete found trojans* (borrar inmediatamente los troyanos detectados), Anti-Trojan no se limitará a notificar la existencia de troyanos. De inmediato emprenderá el borrado automático de los archivos correspondientes.



Aquí fue detectado y erradicado inmediatamente un troyano.

2. Muy importante: si durante la verificación Anti-Trojan detectó y erradicó troyanos, usted deberá reiniciar enseguida el ordenador. De lo contrario, un troyano que aún se encuentre en la memoria de trabajo podría volver a infectar el PC.



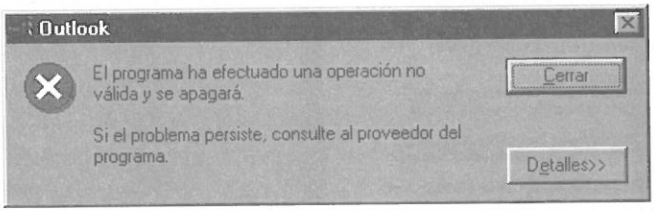
Una vez erradicado un troyano, hay que reiniciar inmediatamente el ordenador.

3. Tras el reinicio, por precaución debería ejecutar una vez más Anti-Trojan, para asegurarse de que el troyano ha desaparecido realmente.

Cuarentena – verificar cuidadosamente el software nuevo

Examinar un programa nuevo y desconocido nada más descargarlo para ver si contiene virus, debería ser ya algo incuestionable. Pero que su escáner antivirus no encuentre nada, aún no significa que estos programas no sean peligrosos para su PC. A fin de cuentas, usted sólo sabe el nombre del programa y las funciones

que se le atribuyen. Sin embargo, por debajo de esto, mientras el software simulara ser una aplicación inofensiva, podría destruir datos en su ordenador o devastar toda la información de su disco duro con una simple intervención en la tabla de particiones. También los troyanos descritos en este capítulo son difundidos así con frecuencia. Además, un programa no tiene por qué causar daños deliberadamente. Quizá sólo haya sido programado chapuceramente, o no fue probado lo suficiente. A lo mejor contiene un error, que sólo tiene consecuencias con determinadas condiciones. Y precisamente en su PC, estas se cumplen. Pero si ocurre algún desastre, ¿le consolaría a usted saber que las probabilidades de que sucediera eran de una entre un millón?



Nobody is perfect – hasta los fabricantes de software importantes producen constantemente aplicaciones defectuosas.

INFO

Llamadas telefónicas a Oceanía

Un buen ejemplo de los daños que puede causar un programa desconocido apareció hace algún tiempo en la prensa. Un sitio web americano ofreció para descarga gratuita imágenes y vídeos de contenido específico. Sin embargo, para bajar esos datos había que instalar un software especial que también era ofrecido sin coste. Un número considerable de clientes lo instaló e intentó acceder con él al servidor del oferente. Sin éxito. La mayoría lo atribuyó a un problema técnico o pensó que le habían tomado el pelo, olvidando el programa instalado. Pero este no estuvo para nada inactivo. En realidad, utilizó los módems existentes para llamar con la máxima frecuencia posible a un número de teléfono de coste elevado (comparable a los números 906 en España o 0190 en Alemania). Los usuarios que repararon en esta constante actividad del módem, fueron los menos. La mayoría no se dio cuenta hasta recibir la siguiente factura de teléfono, con lo que reclamaron indignados a la compañía telefónica. Ésta sólo pudo constatar que los operarios de ese número estaban asentados en algún lugar de Oceanía y no podían ser hechos responsables del daño causado. Los clientes estafados se quedaron con un palmo de narices.

Más sobre troyanos y parásitos similares:
http//members.ncbi.com/mewolf1/troyanos.html

Para protegernos de estos lobos con piel de cordero, el primer recurso disponible es la prevención. Antes de instalar un software desconocido, infórmese sobre sus funciones. Si por ejemplo un amigo suyo ya lo tiene instalado y no ha detectado ningún efecto negativo, usted también podrá arriesgarse. Lo mismo vale para los programas presentados en revistas o libros de informática. También en

este caso, podrá confiar en la pericia de los expertos. Pero asegúrese de utilizar la misma versión de software que ellos recomienden. Las anteriores o las más recientes podrían contener pese a todo, errores peligrosos.

Si usted quiere probar a todo trance una aplicación sin saber gran cosa sobre ella, debería vigilar el software durante el primer arranque y someterlo a pruebas exhaustivas. Sólo así podrá estar seguro de que ese programa hace en su ordenador sólo lo que tiene que hacer. En el siguiente workshop (taller) vamos a mostrarle el mejor modo de hacerlo.

TRUCO

Un segundo sistema operativo para hacer pruebas

Si usted desea probar regularmente nuevos programas y no quiere molestarse cada vez con backups y riesgos de seguridad, puede emplear el siguiente truco: instale en su PC una segunda versión del sistema operativo, que esté totalmente separada de la primera en otra partición o disco duro. En este sistema de test, pruebe exhaustivamente el nuevo software antes de incluirlo en el entorno de trabajo real. También puede aprovecharse de esta técnica. Todo lo que necesita es una partición libre en su disco duro o quizá, un segundo disco duro además de un administrador de arranque, que le permita elegir entre un sistema operativo y el otro.

Verificar programas desconocidos en el cajón de arena

Para testear un software desconocido e impedirle al mismo tiempo que cause daños a su ordenador, debe encerrar a esa clase de programas dentro de un cajón de arena virtual (sandbox). Este es un sistema especial que vigila todos los componentes y recursos del PC e impide accesos ilícitos. Simultáneamente, el sistema registra esos accesos y se los comunica a usted. De este modo, cuando comprueba un software nuevo puede saber, en todo momento, a qué recursos acceden los programas desconocidos. A poco que sepa sobre su sistema, usted mismo podrá decidir si esos accesos están dentro de la zona verde o suponen una amenaza para su ordenador.

INFO

Los recursos de su ordenador

El cajón de arena virtual o Sandbox controla y protege los diferentes componentes de hardware y software de su ordenador. Los más importantes podrían ser quizá los discos duros con su sistema de archivos. El cajón de arena puede ser ajustado de tal modo, que sólo permita al programa nuevo el acceso a directorios muy concretos. Como mínimo, debería estar permitido el acceso con lectura al propio directorio de programas. Para el primer test, habría que desactivarles a muchos programas los accesos con escritura. Un punto crítico son las ampliaciones de hardware para los vínculos online, es decir, los módems, adaptadores RDSI o tarjetas de red. De éstas pueden abusar los troyanos para transmitir datos confidenciales. Los módems y las tarje-

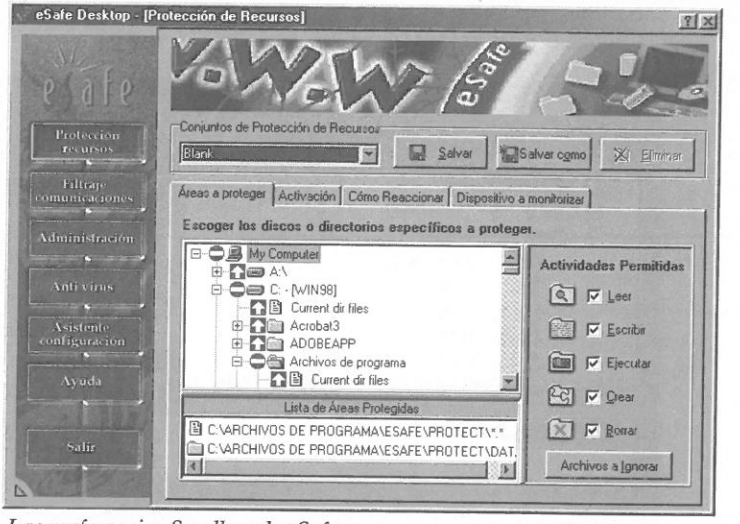
tas RDSI aún permiten extraer temporalmente la clavija del teléfono. En las tarjetas de red, esto resulta menos aconsejable. Aquí el cajón de arena debería interceptar y bloquear los accesos. Pero también los componentes de software, como son los archivos de registro, deben ser protegidos de accesos demasiado entusiastas.

En el siguiente taller queremos mostrarles cómo funcionan estos sistemas de cajón de arena. Para ello, vamos a recurrir al programa *eSafe*, cuya instalación y manejo se describen en el Capítulo 4, bajo el apartado sobre los firewalls. Aparte de un firewall, este programa también incluye numerosas funciones de seguridad adicionales entre las que se cuenta un sandbox o cajón de arena virtual para comprobar software desconocido. En nuestro taller, vamos a suponer que usted ya ha instalado eSafe en su ordenador y lo tiene activado.

El cajón de arena virtual está compuesto por un conjunto de reglas, que describe lo que un programa puede hacer y lo que no. Antes de arrancar un programa nuevo por primera vez, usted debe definir este conjunto de reglas.

1. Abra para ello el apartado *Sandbox* en la barra de navegación del menú de configuraciones de eSafe. De modo similar a las configuraciones del firewall, también aquí encontrará arriba del todo un área para administrar los conjuntos de reglas. Si quiere testear una aplicación con seguridad, sólo debe crear un conjunto de reglas para esa aplicación (o recurrir a uno de los conjuntos de reglas predefinidos).

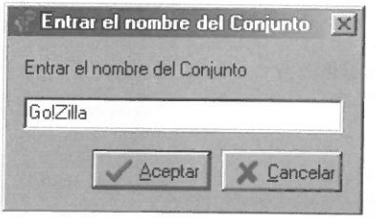
Conjunto de reglas predefinido	Ámbito de aplicación
Blank	El conjunto de reglas "vacío" permite todo tipo de accesos y sólo protege de manipulaciones al directorio eSafe.
Freeze Desktop	"Congela" el escritorio de Windows, es decir, las aplicaciones no podrán modificar ni el menú de inicio ni el escritorio.
Internet Applications	Protege de los peligros procedentes de Internet. Sólo se permiten accesos a los directorios típicos para aplicaciones de Internet. Se impide a nivel general la creación de archivos script potencialmente peligrosos.
Internet Explorer	El conjunto de reglas especial para Internet Explorer permite acceder sólo a las áreas donde este navegador tenga algo que buscar. Además, se impide la creación de archivos script en todos los drives.
Netscape	El conjunto de reglas especial para Netscape Navigator tiene la misma función que el de Internet Explorer.
Untrusted Applications	El conjunto de reglas para aplicaciones sospechosas restringe las posibilidades de acceso para las aplicaciones a unos pocos directorios de test y de descarga, así como a la carpeta temporal. Además, queda bloqueada la creación de archivos script potencialmente peligrosos.



Las preferencias Sandbox de eSafe.

2. Para generar un nuevo conjunto de reglas, seleccione en primer lugar el conjunto vacío *Blank* en la lista de conjuntos de reglas.

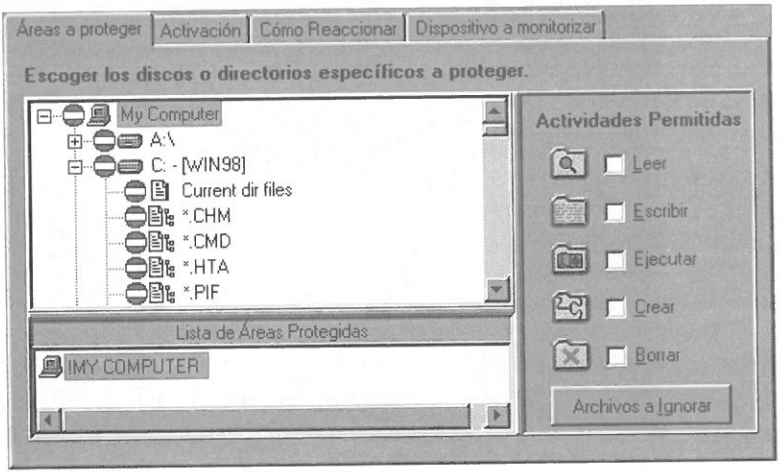
3. Guarde este conjunto con el botón *Salvar como*, asignándole nombre apropiado en la ventana de nombre de conjunto (por ejemplo el de la aplicación que se vaya a analizar). Si fuera necesario, confirme el mensaje de advertencia sobre la creación de conjuntos de datos independientes de la aplicación.



Así se guarda un nuevo conjunto de reglas.

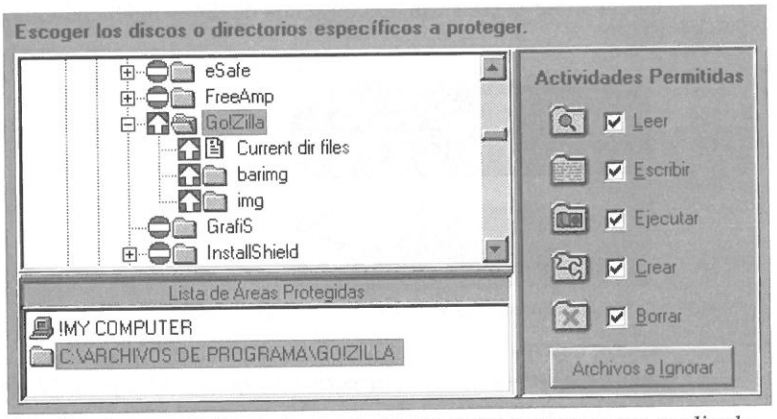
Ahora, hay que rellenar el nuevo conjunto con reglas. Para eso, en el apartado *Escoger los discos o directorios específicos a proteger* puede establecer con exactitud a qué datos tendrá acceso el nuevo programa. Lo normal sería bloquear por principio todos los discos y directorios, con la única excepción del directorio donde se aloje el propio programa. Aquí, debería permitirse el acceso a archivos de configuración y el almacenamiento de datos temporales. Lo mejor será que proceda del siguiente modo:

4. Seleccione primero *My Computer* y para éste, desactive en el área *Actividades permitidas* todos los derechos de acceso.



Desactive primero todos los derechos de acceso para la totalidad de las zonas.

5. Elija ahora el directorio donde esté instalado el programa que vaya a ser comprobado y vuelva a autorizar en él todos los derechos. Así, el programa al menos podrá moverse libremente dentro de su propio directorio, donde a fin de cuentas poco daño podrá hacer.



Autorice al menos el directorio propio del programa que vaya a ser analizado.

TRUCO

Autorizar otros directorios

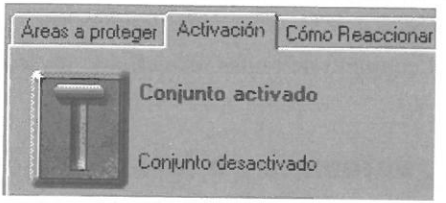
Muchas veces resulta lógico autorizar más directorios. Por ejemplo, muchas aplicaciones necesitan acceder a la carpeta temporal de Windows para almacenar allí provisionalmente archivos. Debido a su ámbito de aplicación, algunos programas requieren acceso a determinados directorios. Un programa de administración de cookies (véase también el Capítulo 8), por ejemplo, necesita acceder sin falta a la carpeta de cookies para poder funcionar. Pero estas ampliaciones las puede hacer usted poco a poco, cuando el test del programa le vaya aclarando los archivos concretos a los que quiera acceder la aplicación. Si éstos son inofensivos, cambie las reglas para autorizar el acceso a los mismos y testee el programa de nuevo.

6. Cambie ahora a la pestaña *Activación*, para decidir si el conjunto de reglas es válido y para qué programas. En la parte superior, determine primero si debe estar *Sandbox activo* para este conjunto de reglas; si quiere utilizar el conjunto de reglas en *Modo de aprendizaje*, o si *no quiere emplear sandbox*. Con esto podrá desconectar temporalmente conjuntos independientes cuando lo necesite.

INFO

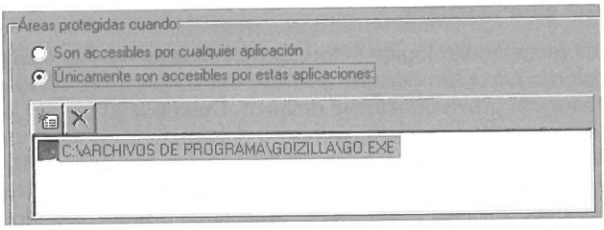
El modo de aprendizaje de eSafe

En el modo de aprendizaje, eSafe registra todos los accesos de la aplicación y sobre esta base, él mismo define las reglas para esos programas. Pero esto sólo tiene sentido si usted está seguro de que la aplicación no supone ningún riesgo. Este modo permite, por ejemplo, generar conjuntos de reglas para software de desarrollo propio y difundirlos con el software. Para ello, usted puede seleccionar el modo de aprendizaje en la pestaña *Activación*, de las configuraciones de sandbox, e indicar hasta qué fecha deberá mantenerse la fase de aprendizaje (por regla general un mes). Una vez transcurrida esta fase, será cerrada automáticamente y el conjunto de reglas generado hasta entonces se activará.



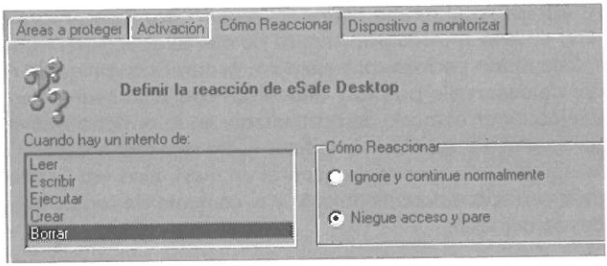
Active sandbox para el conjunto de reglas que quiera crear.

7. Ahora, en la zona *Áreas protegidas cuando*: defina para qué aplicación deberá regir ese conjunto de reglas. Escoja la opción *Únicamente son accesibles por estas aplicaciones* y haga clic sobre el botón *Añadir*, situado en la parte superior izquierda. En el diálogo de selección de archivos que aparecerá a continuación, elija el archivo de programas de la aplicación que quiera analizar.



Seleccione la aplicación para la que deba regir el nuevo conjunto de reglas.

8. Cambie a continuación a la categoría *Cómo reaccionar*, para decidir cómo debe reaccionar eSafe ante violaciones de las reglas por parte del programa a examen. Cuando pruebe nuevo software, debería *negar y parar el acceso* en caso de cualquier tipo de infracciones de protección. Es imprescindible mantener activos los avisos, es decir, NO elija la opción *Sin aviso*, para que durante el test de la aplicación pueda ser advertido inmediatamente de las violaciones de protección. De lo contrario, es posible que la aplicación que está bajo test se interrumpa sin comentarios tras haberle impedido eSafe determinado acceso. Pero en este caso, usted no sabría si esa caída se debe a una reacción de eSafe o a un fallo del propio programa.



Establezca reacciones severas ante las infracciones de protección.

9. Finalmente, guarde el conjunto de reglas así definido haciendo clic sobre *Guardar.*

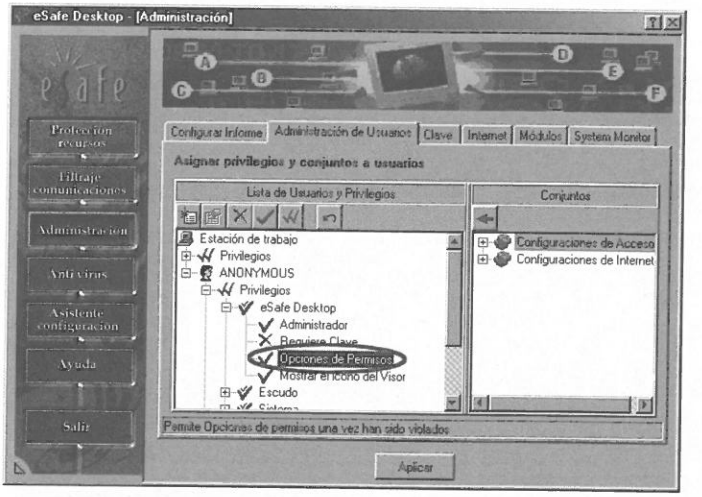
Modo de prueba: ¿automático o interactivo?

Antes de comenzar el test en sí, usted debería decidir un método de prueba. Por regla general, el test se desarrolla en modo automático, que impide o bloquea las violaciones de reglas en función de las configuraciones previas. Aparecerá (también según las configuraciones previas) una advertencia, o la reacción de eSafe será registrada en un protocolo. Existe una alternativa a esto: el modo interactivo. Dentro de este modo, será advertido cada vez que se produzca una violación de las reglas y podrá decidir si eSafe debe permitir o bloquear la acción. Este modo resulta especialmente indicado cuando se dan los primeros pasos con un

nuevo programa. Así, se puede comprobar rápidamente a qué recursos necesita acceder obligatoriamente la aplicación para poder funcionar. La autorización interactiva de accesos inofensivos evita tener que adaptar constantemente la regla.

1. Para ajustar el modo de test interactivo, abra las configuraciones de administración de eSafe y una vez allí, cambie a la categoría *Administración de usuarios.*
2. Ahora, abra para el usuario con el que se vaya a analizar la aplicación, la subpropiedad *Privilegios/eSafe Desktop.*
3. Aquí encontrará, entre otras, la propiedad *Opciones de permisos* que podrá activar con un doble clic (de modo que quede precedida de una marca verde). Esto pone en marcha el modo interactivo para las violaciones de protección.
4. A continuación, *aplique* la nueva configuración para los usuarios.

En el Capítulo 2, se describe con detalle el administrador de usuarios de eSafe. Si hasta ahora aún no había empleado ese componente de eSafe, en la lista de usuario sólo le aparecerá el usuario *Anónimo* (Anonymous). Éste as asignado automáticamente a todos los usuarios para los que no exista ningún otro perfil. En este caso, usted debería activar para ese usuario la propiedad *Opciones de permisos.*



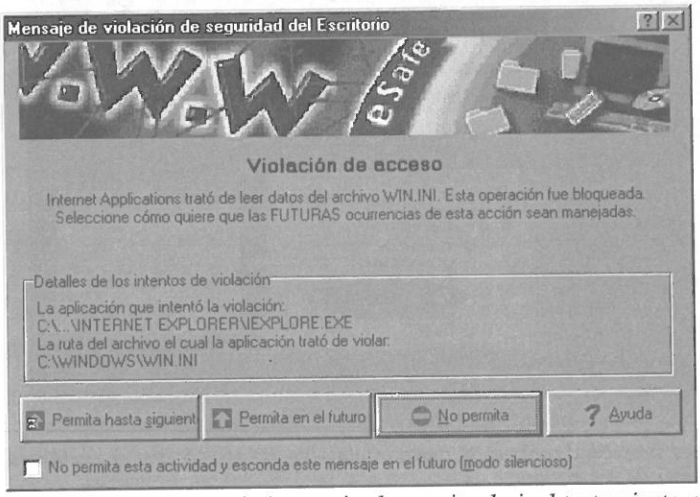
Esta propiedad controla el modo interactivo, en caso de que se produzcan violaciones de protección.

El test de la aplicación

Ahora hay que probar el programa. Antes de nada, vuelva a asegurarse de que el nivel de seguridad de eSafe está en *Normal* o, mejor aún, en *Extremo*. Sólo entonces actuarán de verdad las restricciones definidas. Arranque después el programa y sométalo a un test exhaustivo. Esto implica, aparte del uso de las funciones principales, la prueba de todas las funciones secundarias si es posible, y quizá de los programas auxiliares integrados. Es importante que la aplicación sea ejecutada durante un tiempo prolongado. Las aplicaciones cuyo gestor de memoria fuera programado descuidadamente, suelen interrumpirse sin razón aparente cuando ya ha transcurrido algún tiempo. Si usted dispone de tiempo, lo mejor sería ampliar la fase de prueba a varios días o semanas.

Violaciones de las reglas por el programa analizado

Mientras se ejecuta el programa, eSafe vigila todas sus actividades. Si arranca un acceso que va en contra de las reglas de protección formuladas, el programa se detendrá y un mensaje le advertirá a usted de la incidencia. En el modo automático, este mensaje sólo le informa de la aplicación que quiere acceder sin permiso y a qué archivos, pero tras haber sido bloqueada ya la acción de esa aplicación. En muchos casos, este bloqueo trastorna a la aplicación, que ya no se seguirá ejecutando correctamente. El modo interactivo le facilita, además, varias opciones para enfrentarse a esa violación de protección. Con algunos conocimientos, usted mismo puede juzgar si el acceso en cuestión supone un peligro o no. Puede reaccionar de varias maneras:



Un mensaje de advertencia interactivo le permite elegir el tratamiento que debe recibir la violación de protección.

- *Permita hasta siguiente* le proporciona acceso provisional hasta que se arranque de nuevo el ordenador. Pero las reglas existentes no son cambiadas de modo permanente, de manera que si se vuelve a intentar el mismo acceso, se producirá otra vez la violación de protección. Elija esta opción si el acceso no supone ningún peligro directo pero usted no puede excluir un riesgo general.
- *Permita en el futuro* autoriza el acceso ahora y también en el futuro. Es decir, el programa de test podrá acceder desde ahora a los datos, sin que se produzca ninguna violación de protección. eSafe hace esto adaptando automáticamente las reglas de protección. En resumen, si usted permite aquí el acceso a un determinado directorio, será modificado también el conjunto de reglas automáticamente.
- *No permita* impide totalmente el acceso. Elija esta opción siempre que tenga dudas sobre un acceso. Generalmente, el programa bajo test reaccionará con un mensaje de error. Pero también puede ocurrir que el programa no funcione bien sin este acceso y provoque una caída del sistema. Aquí, lo importante es encontrar el término medio entre seguridad y rendimiento.
- Para que el mismo acceso no esté provocando constantemente un mensaje de error, cuando vuelva a aparecer dicho mensaje, si lo desea podrá activar la casilla *No permita esta actividad y esconda este mensaje en el futuro.* Así, un acceso que haya sido prohibido una vez, en el futuro será bloqueado siempre sin comentarios.

Cómo reaccionar ante accesos ilícitos

Si un programa sometido a prueba está empeñado en dedicarse a la caza furtiva en cotos ajenos, es decir, pretende acceder a directorios y archivos con los que en realidad no tiene nada que ver, usted deberá decidir si se lo permite o no. Para ello, el criterio más importante debería ser el archivo que el programa quiera leer o modificar. eSafe le comunicará el nombre del mismo. Intente reconocer por el nombre, de qué archivo se trata. Si lo conoce, podrá juzgar usted mismo si desea autorizar el acceso o no. Si no sabe el contenido del archivo solicitado, lo mejor será que impida el acceso por si acaso.

Las funciones del modo interactivo le permiten a entrenar poco a poco (no confunda esto con el modo de aprendizaje) el conjunto de reglas de protección para cada programa. En cada acceso permitido o prohibido a largo plazo, eSafe adapta el conjunto de reglas. Si el programa se ejecuta sin mensajes de advertencia y cumple correctamente su cometido, se puede suponer que el conjunto de reglas es correcto y le proporciona a usted una protección fiable sin limitar al programa. Si por el contrario, un programa intenta acceder repetidamente a directorios y archivos con los que en realidad no tiene relación, usted debería replantearse

si de verdad quiere emplear este programa. Pero aun así, no hay motivo de preocupación. Mientras eSafe esté activo, impedirá el acceso no deseado y usted podrá estar tranquilo.

4. Nivel de seguridad 3: protección contra intrusos

4.1 **Un muro de protección contra los atacantes – firewalls** 203
Principio funcional: filtraje regulado del tráfico de datos 204
Soluciones profesionales frente a los firewalls personales 206
Sencillo y seguro: ZoneAlarm, para usuarios noveles 207
Flexible y potente: eSafe para usuarios avanzados 221

4.2 **La confianza está bien, el control aún mejor – vigilar el ordenador** 248
Controlar los ataques y otras actividades 249
Vigilancia automática de PCs no custodiados 259

En los capítulos precedentes, nos hemos ocupado, sobre todo, de la protección pasiva. Es decir, de la configuración y utilización segura del sistema y del cierre de agujeros de seguridad peligrosos. Ahora, vamos a asumir un papel más activo y a tomar medidas que incrementen aún más la seguridad de nuestro PC y de los datos que contiene. Esto requiere un software que incluya funciones de seguridad adicionales. Programas de este tipo son los firewalls, que vigilan todos los datos que fluyen entre el PC e Internet. Para ello, emplean filtros que sólo permiten el paso de determinados tipos de datos. También existe la posibilidad de filtrar el contenido, es decir, no autorizar la salida ni entrada de datos con determinado contenido. Aparte de este aislamiento técnico del PC ante la red, habría que vigilar al propio ordenador para evitar intervenciones y ataques. Existen programas especiales que permiten protocolar automáticamente todo lo que ocurre en el ordenador durante la ausencia de su dueño. De este modo, se pueden descubrir rápidamente los robos disimulados de datos.

4.1 Un muro de protección contra los atacantes – Firewalls

Todos los PCs conectados a Internet emplean para la comunicación el protocolo TCP/IP y otros modelos basados en él. Esto funciona sin importar si los ordenadores están conectados permanentemente a Internet, o sólo enlazan por conexión telefónica cuando lo necesitan, ya sea vía módem o RDSI. TCP/IP es una familia de protocolos enfocada a la eficacia, pero no a la seguridad, por lo que ofre-

ce a los hackers multitud de posibilidades de ataque para espiar o paralizar los ordenadores ajenos.

INFO

¿Qué significa TCP/IP?

TCP/IP es el protocolo de comunicaciones más importante de Internet. Consta exactamente de dos componentes: el *Transmission Control Protocol* (TCP) y el *Internet Protocol* (IP). El *Transmission Control Protocol* (TCP) fracciona la información en paquetes manejables, éstos a su vez son transmitidos por *Internet Protocol* (IP) al ordenador destinatario, donde son reconvertidos por TCP a la información original. Ambos protocolos son independientes de la plataforma, por lo que cualquier ordenador o programa puede intercambiar datos a través de la Red. Todos los protocolos de Internet de orden superior, como *Hypertext Transfer Protocol* (HTTP) para la *World Wide Web* (WWW) o *Simple Mail Transfer Protocol* (SMTP) para el correo electrónico, se basan en las funciones de TCP/IP. Cuando se desarrolló TCP/IP, se buscó, ante todo, eficacia y flexibilidad. Los paquetes de datos abren por sí mismos el camino más corto, evitando automáticamente las áreas de la Red que se encuentren sobrecargadas o caídas. Mientras exista cualquier conexión entre el ordenador de salida y el ordenador objetivo, existe una gran probabilidad de que los datos alcancen su objetivo. El entorno en el que se pensó a la hora de desarrollar TCP/IP, era una red mundial que debía permitir la comunicación, incluso tras una guerra nuclear. Pero no se tuvieron en cuenta los ataques desde el interior, como por ejemplo los que se lanzan contra los puntos débiles en la seguridad de los protocolos.

En consecuencia, para protegerse de ataques desde Internet es necesario aislar el ordenador. Naturalmente, el mejor modo sería el puramente físico, es decir, extrayendo la clavija de conexión a la Red. Pero, como entonces tampoco el PC estaría ya en contacto con la Red, esta solución resultaría quizá demasiado radical. En realidad, lo que se necesita es una "clavija inteligente", que sólo permita el tráfico de datos deseado e impida el resto. Cosa que no es vana ilusión, sino algo totalmente factible. La palabra mágica es "firewall".

Principio funcional: filtraje regulado del tráfico de datos

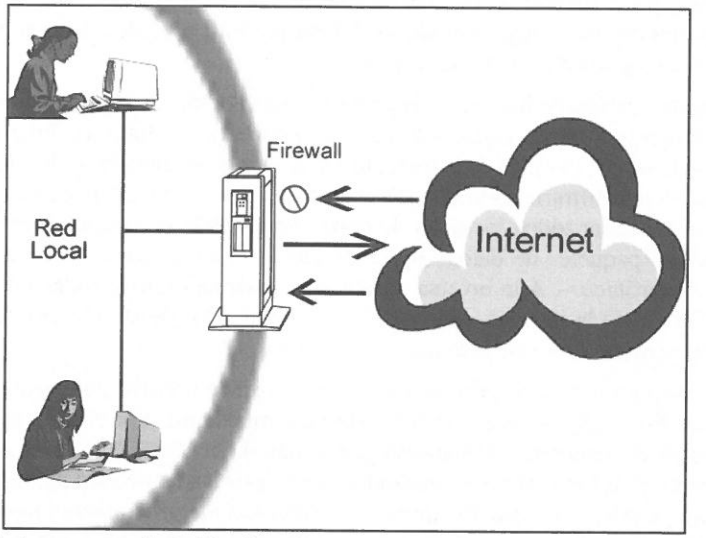
Los protocolos TCP/IP trabajan por paquetes, es decir, todos los datos a transmitir son fraccionados en pequeños paquetes. Cada uno se compone de diversa información de control, como la dirección IP del ordenador remitente y de la máquina de destino, además del contenido en sí. Si usted, por ejemplo, solicita a un servidor web una página web, el servidor descompone el archivo pertinente en multitud de pequeños paquetes, que pondrá en camino hacia la dirección IP de su ordenador. Los paquetes son capaces de buscar el camino solos. Una vez en su PC, el navegador web reúne los diferentes paquetes y los vuelve a componer para formar la página web original.

Antes de que todo esto ocurra, intervienen los llamados firewalls o cortafuegos. Estos mecanismos de protección basados en hardware o software, vigilan todos los paquetes de datos de entrada y salida y son capaces de cribar los paquetes nocivos, antes de que sean recompuestos en sus datos originales y puedan causar daños al ordenador. Estos filtros de paquetes se emplean como interfaz entre un PC o una red local e Internet. Analizan los paquetes de datos y prestan atención:

- a su procedencia,
- a quién van dirigidos,
- al protocolo que emplean y
- a su contenido.

Con una combinación flexible de reglas, se puede decidir a qué paquetes se permite pasar sin problemas y cuáles deben ser rechazados como peligro potencial. De esta forma, se puede:

- rechazar todos los paquetes de datos procedentes de una determinada dirección,
- impedir transmisiones de datos desde el propio ordenador a otros ordenadores concretos,
- impedir el empleo de determinados protocolos o
- rechazar paquetes de datos por contener determinadas palabras clave.



Así protege un firewall ordenadores y redes locales.

INFO

¿Qué significa exactamente firewall?

El término inglés firewall (traducido, viene a significar "muro cortafuegos") procede del ámbito de la prevención de incendios o la ingeniería civil. Antiguamente, en las grandes ciudades ocurría con frecuencia que un incendio, en origen pequeño, destruía bloques de viviendas o incluso barrios completos. Esto se debía a que en las calles de construcción densa, las llamas saltaban enseguida de una casa a otra. Por eso, en algún momento surgió la idea de erigir entre las casas un cortafuegos. Esto es un muro que debe poseer determinado grosor y estabilidad, además de no tener ventanas. Con este tipo de muros, se evita en la mayoría de los casos que el fuego pase a la siguiente casa. Cuando fueron desarrollados los filtros de paquetes para redes, surgió pronto la idea de recurrir a la expresión inglesa firewall, ya que también aquí, se pretende evitar que los peligros y daños se propaguen de una sección de la Red a otra.

Soluciones profesionales frente a los firewalls personales

Hoy en día, la expresión firewall se emplea con relación a diferentes tipos de productos. Inicialmente, los firewalls fueron desarrollados sólo para aplicaciones de redes profesionales, y estaban concebidos casi siempre como hardware. Es decir, había que comprar una caja negra más o menos pequeña y conectarla entre la propia red e Internet. Muchas veces, un módulo firewall va integrado también en una solución de redes más compleja. Así, instalando por ejemplo un nodo de red distribuidor, se pueden establecer a la vez reglas de filtraje; los tipos de paquetes de datos cuya entrada se deberá permitir y cuáles deberán ser bloqueados en alguna de las dos direcciones.

Un cometido típico de los firewalls profesionales podría ser la protección de una red de empresa o intranet que, a su vez, vaya conectada a Internet. En este caso, el firewall sería colocado directamente en el punto de transición del intranet a Internet, donde filtraría todo el tráfico de datos. Un cometido frecuente es, por ejemplo, bloquear todos los tipos de conexiones desde el exterior y permitir el paso sólo a paquetes de datos muy concretos – como pueden ser mensajes de correo electrónico –. A la inversa, también se podrían impedir todas las consultas HTTP desde la intranet a Internet, si los empleados de la empresa no tienen permiso para navegar por Internet.

Estas soluciones firewall profesionales apenas tienen utilidad para usuarios particulares. Por un lado, suelen ser casi siempre muy caras. Por el otro, se requiere un gran esfuerzo para instalarlas y, además, la configuración y el mantenimiento son más bien difíciles. Mirándolo bien, precisamente esto último supone un riesgo añadido, ya que un firewall configurado incorrectamente por falta de conocimientos, mantendría al usuario en un estado de seguridad engañoso.

Por ello, para proteger al propio PC, resulta más recomendable un producto del ámbito de los "firewalls personales". Por lo general, son productos de software que se instalan como complemento del sistema operativo. Trabajan según el mismo principio básico, sólo que se encajan directamente en el protocolo TCP/IP del sistema operativo e instalan allí sus filtros. Resultan mucho más baratos y, sobre todo, son mucho más fáciles de manejar por haber sido concebidos para el usuario normal. Así, no hace falta pelearse con la formulación de definiciones de paquetes de filtros, cosa compleja y susceptible de traer errores. Por el contrario, se puede seleccionar fácilmente desde una superficie de cómodo manejo, qué servicios Internet deben estar disponibles, qué aplicaciones pueden acceder a Internet y qué datos deben ser protegidos selectivamente de una transmisión a Internet.

A continuación, vamos a presentarle dos productos diferentes dentro del entorno de los firewalls personales. En primer lugar, mostraremos un programa que puede ser instalado y activado con gran rapidez y sin complicaciones, por lo que resulta especialmente indicado para usuarios noveles que quieran ir a lo seguro. Después, queremos familiarizarle con un producto algo más complejo, que requiere un mayor esfuerzo a la hora de instalarlo y mantenerlo. En contrapartida, usted será recompensado con una herramienta más eficaz y flexible, que se deja adaptar óptimamente a las necesidades individuales de protección.

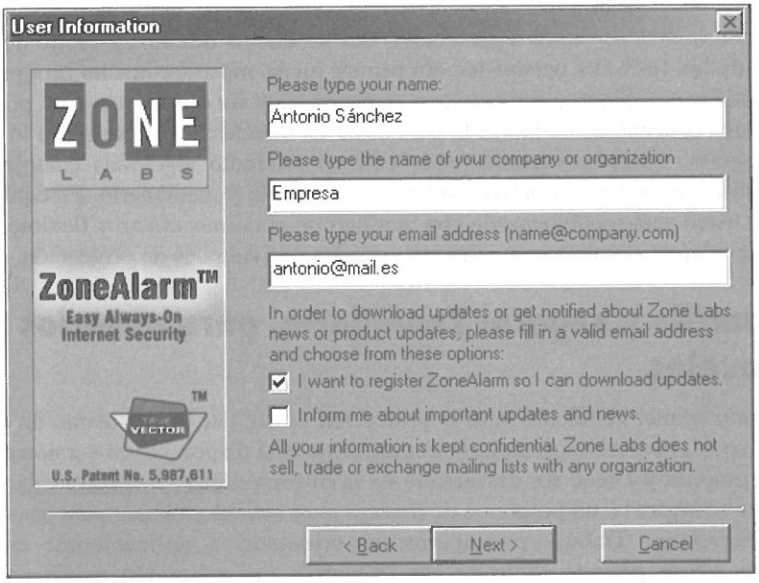
Sencillo y seguro: ZoneAlarm, para usuarios noveles

Como primer candidato para la protección eficaz del PC mediante un firewall personal, queremos presentarle *ZoneAlarm*. Está disponible en versión de prueba gratuita y puede ser descargado de la dirección http://www.zonealarm.com. Este software es un programa de manejo muy sencillo, idóneo para usuarios sin experiencia. Trabaja principalmente orientado a aplicaciones, es decir, ZoneAlarm permite controlar con exactitud qué aplicación puede acceder a Internet y de qué manera. Esto brinda una protección altamente fiable contra troyanos y malhechores ocultos de la misma índole. Aparte de eso, también se puede desactivar totalmente el tráfico de datos entre el PC e Internet con un simple clic del mouse. Asimismo, unas configuraciones automáticas hacen que el programa resulte interesante para todos aquellos que estén permanentemente vinculados a Internet a través de una red local, o aquellos que se conecten mucho tiempo a Internet por conexión telefónica de tarifa plana.

Instalar ZoneAlarm

La instalación de ZoneAlarm es sumamente sencilla. Tal y como nos tienen habituados las aplicaciones modernas de Windows, un cómodo asistente nos guiará a través de todo el proceso de instalación. En principio, sólo es necesario

confirmar el acuerdo de licencia y seleccionar la carpeta para la instalación de los archivos. Únicamente hay que prestar atención a la introducción de la *User Information*, la información sobre el usuario. Aquí podrá introducir su nombre y su dirección de correo electrónico. Si aparte de esto, usted activa la opción *I want to register ZoneAlarm so I can download updates*, el programa le registrará vía Internet la primera vez que inicie la sesión. Así, en el futuro podrá bajarse automáticamente las actualizaciones de ZoneAlarm e integrarlas. Si piensa utilizar el programa durante mucho tiempo, esto es sin duda muy recomendable. De hecho, los programas firewall tampoco están absolutamente libres de fallos de programación y agujeros, por lo que deberían ser mantenidos siempre al día.

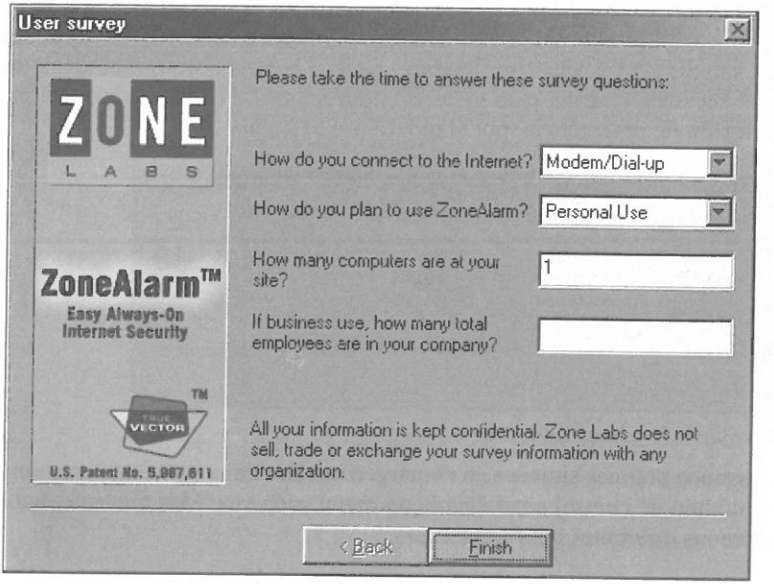


Regístrese como usuario para poder disfrutar de las actualizaciones.

Una vez concluida la instalación, el programa puede ser utilizado enseguida, ya que ni siquiera exige reiniciar el ordenador.

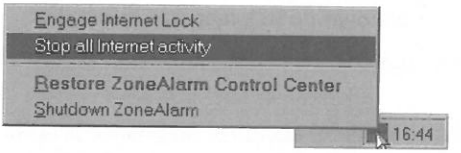
El primer arranque

Durante el primer arranque, que normalmente tiene lugar nada más terminar la instalación, será necesario rellenar, una sola vez, un formulario donde se le harán algunas preguntas breves. Estos datos serán transmitidos a través de Internet al servidor del operador donde, según declara ZoneAlarm, recibirán tratamiento confidencial. Tenga en cuenta que debe rellenar (como sea) todos los campos, antes de hacer clic sobre el botón *Finish* (terminar).



Durante el primer arranque deberá contestar algunas preguntas.

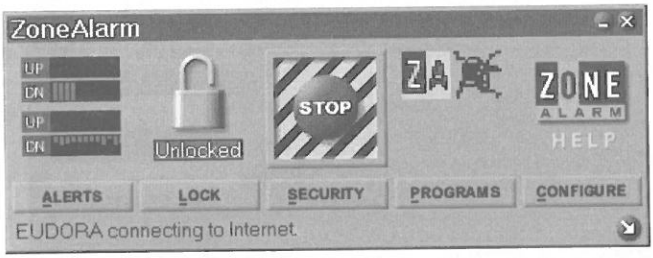
A continuación, verá el símbolo de ZoneAlarm en la parte inferior derecha de la barra de tareas. Este icono indica el estado de seguridad de su ordenador y, aparte de eso, permite el acceso a todas las configuraciones y funciones de ZoneAlarm. Basta con hacer clic sobre el símbolo con la tecla derecha del mouse para abrir el menú contextual de ZoneAlarm. Más adelante, explicaremos el significado de las diferentes funciones.



A través del icono de ZoneAlarm se puede acceder a todas las funciones del programa.

Para abrir el módulo de control central de ZoneAlarm, basta con hacer doble clic sobre el icono de ZoneAlarm con la tecla izquierda del mouse. Aparecerá una pequeña ventana, que informa del estado de seguridad y, al mismo tiempo, permite acceder a la configuración del programa. Los cuatro indicadores horizontales de la izquierda, muestran el tráfico de datos que ZoneAlarm esté vigilando en ese momento. A la derecha, el gran símbolo de un candado aclara si en ese momento el PC está aislado de Internet (candado cerrado – *Locked*) o si existe la posibilidad de establecer conexiones con la Red (candado abierto – *Unlocked*). Este estado puede ser controlado utilizando el interruptor rojo STOP

situado en el centro de la ventana. Por cierto, el estado *Unlocked* no equivale a inseguridad; es el estado de funcionamiento normal que permite a las aplicaciones seleccionadas acceder a Internet. *Locked* por el contrario, bloquea totalmente el acceso a Internet para todas las aplicaciones. Podría decirse que es la desconexión de emergencia, por si quiere ir a lo seguro.



El módulo de control central de ZoneAlarm.

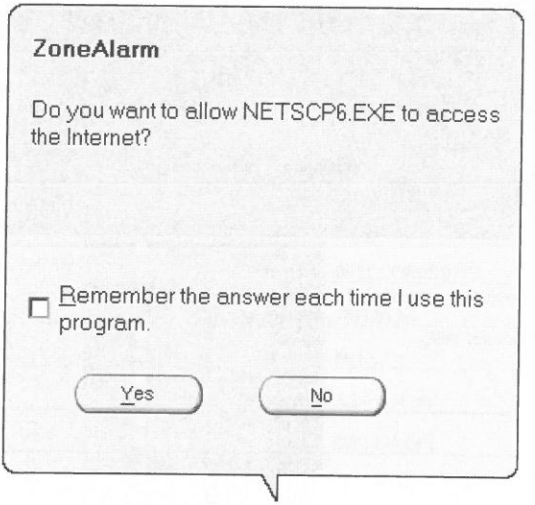
Los cinco botones situados en el margen inferior de la ventana, permiten ampliar el módulo de control añadiéndole un menú cada vez. Más adelante, hablaremos sobre las diferentes configuraciones.

Controlar las aplicaciones con ZoneAlarm

Si ZoneAlarm está activo, controlará automáticamente el flujo de datos entre el PC e Internet. Cada vez que una aplicación intente acceder a Internet, ZoneAlarm lo detectará. Según la configuración, ahora podrá producirse una reacción totalmente automática o una interactiva.

Si ZoneAlarm se topa con una aplicación que el programa aún no conozca, hará una consulta interactiva al usuario, comunicándole qué aplicación pretende acceder a Internet. Usted podrá reaccionar de tres maneras diferentes:

1. Si cree que la aplicación es inofensiva, podrá permitir el acceso haciendo clic sobre Yes.
2. Con un clic sobre *No* puede impedir el acceso si no conoce la aplicación, o no está seguro de si el intercambio de datos está exento de peligro.
3. Si antes de hacer clic sobre uno de los dos botones activa la opción *Remember the answer each time I use this program*, ZoneAlarm recordará la decisión que se tome para esa aplicación. Cuando se inicie la próxima vez el mismo programa, ya no se volverá a lanzar un mensaje de consulta. ZoneAlarm procederá automáticamente según la respuesta dada por usted anteriormente. Así, las funciones de seguridad pueden ser automatizadas y organizadas con mayor comodidad.



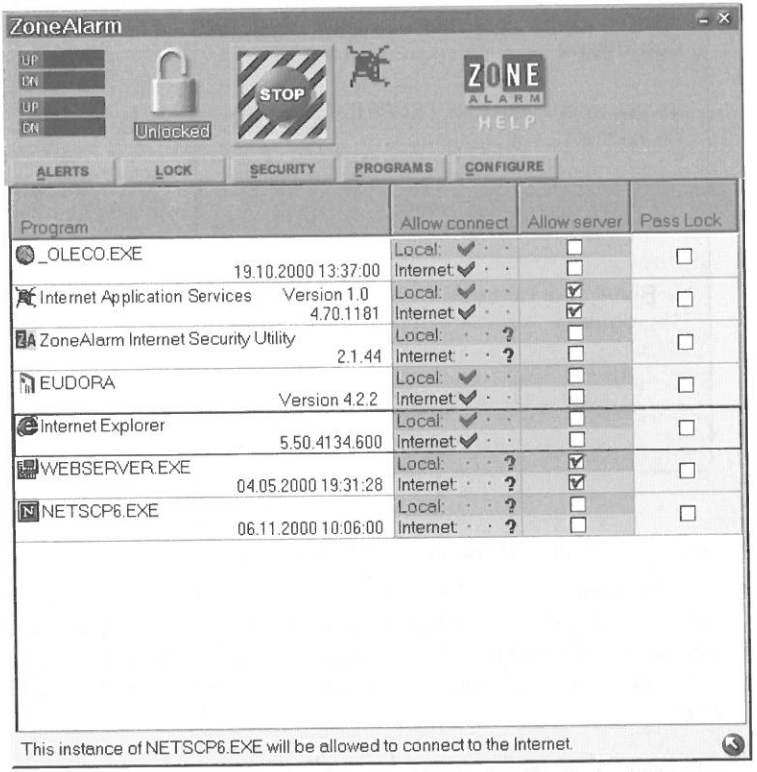
ZoneAlarm impide el acceso de una aplicación a Internet.

De esta manera, ZoneAlarm le permite automatizar poco a poco el control de todas sus aplicaciones de Internet. Si después de eso, alguna vez vuelve a aparecer una ventana de advertencia, podrá deberse a la instalación de un nuevo programa de Internet, o a que de algún modo se ha colado un caballo de Troya en su PC.

Gestionar las reglas para las aplicaciones

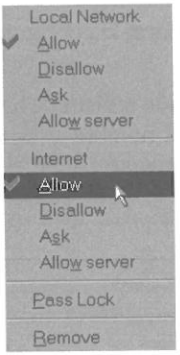
Las reglas de acceso definidas para los diferentes programas en el modo interactivo, pueden ser modificadas posteriormente. Si, por ejemplo, usted denegó equivocadamente el acceso a Internet a una aplicación, podrá anular rápidamente este ajuste y emplear la aplicación.

1. Para ello, abra en el módulo central de ZoneAlarm la configuración de programas, haciendo clic sobre *Programs*.
2. Aquí encontrará una entrada para cada aplicación registrada hasta ahora por ZoneAlarm. Esta entrada contiene, aparte del nombre y la versión de la aplicación, todas las reglas vigentes en ese momento para dicha aplicación.



ZoneAlarm guarda reglas de acceso para todas las aplicaciones de Internet.

3. Si quiere cambiar las reglas para una de las aplicaciones, haga clic con la tecla derecha del mouse sobre la correspondiente entrada. Así, abrirá un menú contextual, que le permitirá definir directamente todas las reglas.



El menú contextual para definir las reglas de acceso.

4. En primer lugar, dentro del menú contextual, podrá decidir por separado para la red local (*Local Network*) y para *Internet* si el acceso de la aplicación debe estar permitido (*Allow*) o prohibido (*Disallow*), o si tendrá que ser autorizado cada vez mediante consulta interactiva (*Ask*). Además, se le permitirá definir si la aplicación puede actuar en la respectiva zona como servidor (*Allow server*).

5. Puede ser de gran importancia la configuración *Pass lock*, que también permite ser ajustada individualmente para cada aplicación. Permite a una aplicación el acceso a Internet, aunque en realidad el acceso general a Internet esté bloqueado por ZoneAlarm (por el gran botón rojo de Stop). Pero recomendamos hacer un uso moderado de este permiso excepcional, ya que minaría el concepto de seguridad de Zone Alarm.

6. Finalmente, con la función *Remove* puede eliminar definitivamente aplicaciones concretas de la base de datos de ZoneAlarm. Esto tiene sentido si usted ha desinstalado un programa o si para una aplicación, quiere volver a configurar interactivamente las reglas.

Las configuración de las zonas de seguridad

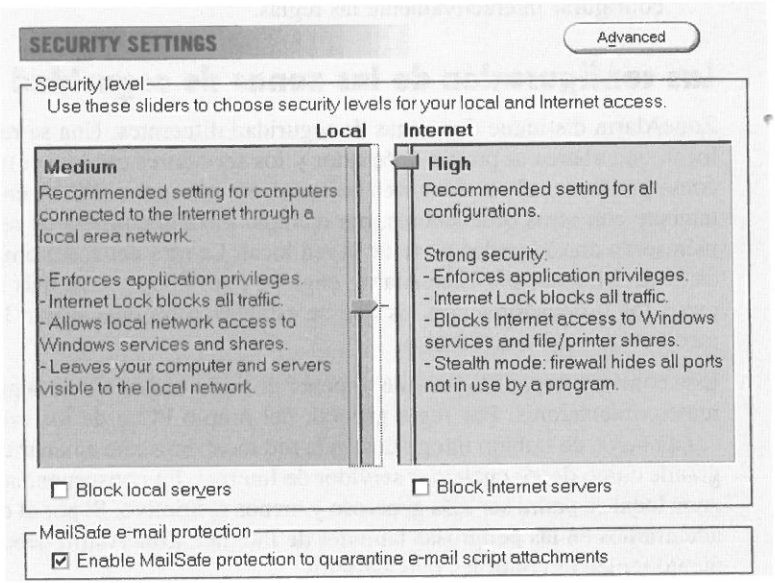
ZoneAlarm distingue dos zonas de seguridad diferentes. Una se refiere a la red local, que abarca al propio ordenador y los servidores que quizá trabajen en él, como podría ser el servidor web personal. Si, además, el PC va enlazado directamente con otros ordenadores, por ejemplo mediante tarjeta de red, éstos también serán considerados parte de la red local. La otra zona, denominada genéricamente *Internet* por ZoneAlarm, engloba todo lo que vaya más allá, es decir, todos los ordenadores con los que se establezca un enlace por TCP/IP, quizá mediante conexión telefónica.

Este concepto bipartido permite imponer distintos requisitos de seguridad a diferentes ordenadores. Por regla general, del propio PC o de los ordenadores de compañeros de trabajo integrados en la red local, no suele emanar un peligro tan grande como desde cualquier servidor de Internet. En consecuencia, dentro de la zona local se podrá ser más generoso y menos restrictivo. Si por el contrario, nos adentramos en las peligrosas latitudes de Internet, ZoneAlarm debería estar más atento y ejercer controles más estrictos.

1. Para ajustar la configuración de las distintas zonas de seguridad, dentro del módulo de control central de ZoneAlarm, haga clic sobre el botón *Security*. ZoneAlarm ampliará su ventana, incluyendo las configuraciones de seguridad.

2. En la mitad izquierda de la ventana, de color verde, podrá ver las configuraciones para la zona local (*Local*). Con la barra deslizante del centro, podrá aumentar o reducir el nivel de seguridad. La configuración estándar para la zona local es *Medium*. En este nivel se controlan las reglas de la aplicación. Por otro lado, un bloqueo de Internet por ZoneAlarm impedirá todo tráfico de datos. Sin embargo, permitirá acceder a recursos liberados por Windows, como por ejemplo unidades de red e impresoras. Tanto el propio ordenador como los servicios liberados podrán ser vistos en la red local.

3. En la mitad derecha, la de color azul, encontrará los ajustes correspondientes a la zona *Internet*. Aquí, el nivel de seguridad estándar es *High*. Con él, además de aplicarse las medidas de seguridad del nivel medio, también será bloqueado el acceso a los recursos compartidos de Windows, y el firewall ocultará todos los puertos que no estén en uso para no exponer innecesariamente el PC a posibles ataques.



Las configuraciones de seguridad de ZoneAlarm se dividen en una zona local y otra para Internet.

4. Adicionalmente, se puede activar para ambas zonas la opción *Block local servers* o *Block Internet servers*. Estas opciones bloquean para cada zona todos los servicios de servidor que pudiera ofrecer el PC. Importante: esta opción global anula las reglas de aplicación individuales que pudieran existir y con las que usted quizá permitió a determinados programas actuar como servidores.

TRUCO

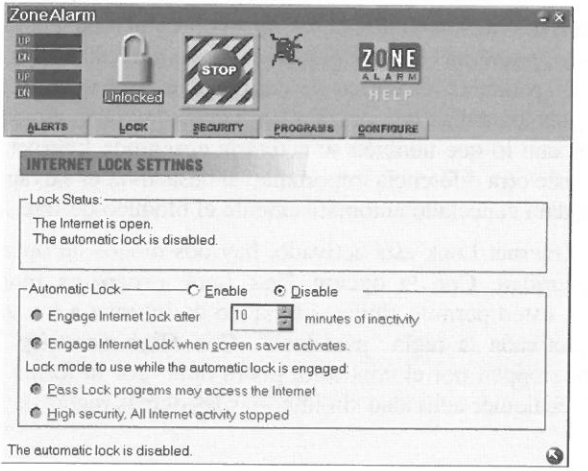
La cuarentena MailSafe

ZoneAlarm ofrece una función de cuarentena para VBS-Scripts potencialmente peligrosos que lleguen a través de correos electrónicos. Esta función es controlada mediante la opción *Enable MailSafe protection to quarantine e-mail script attachments* en las configuraciones de *Security*. Por regla general, esta opción debería estar activada. Aunque en casos aislados, podrían surgir problemas con programas de correo electrónico u otros programas de protección contra virus. En estos casos, debería desconectar esta opción para desactivar la función de cuarentena.

Internet Lock – Bloqueo de Internet

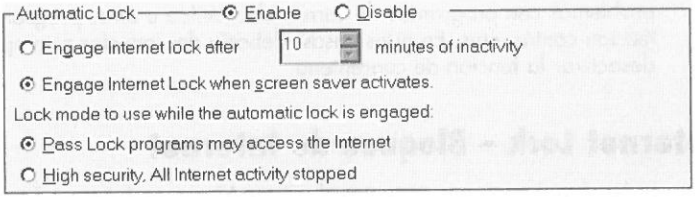
Una de las funciones más potentes de ZoneAlarm es Internet Lock, o bloqueo total del tráfico de datos a través de Internet. Esta función interesa, sobre todo, si la conexión del PC a Internet es regular o prolongada; ya sea de manera permanente por enlace a través de la red local, o al menos de larga duración si usted se conecta a Internet mediante tarifa plana. Ya hemos explicado cómo activar en cualquier momento Internet Lock con el gran botón rojo situado en el módulo de control central de ZoneAlarm. Aunque también existe la posibilidad de activar el bloqueo de Internet automáticamente en determinadas circunstancias. Esto permite mejorar enormemente el estado de seguridad de su PC, sin que tenga que estar pendiente de él a todas horas.

1. Si quiere emprender las configuraciones para el bloqueo de Internet, dentro del módulo de control central de ZoneAlarm haga clic sobre el botón *Lock*. Con esto ampliará la ventana de ZoneAlarm, que ahora incluirá el menú *Internet Lock Settings*.



Las configuraciones estándar para Internet Lock de ZoneAlarm.

2. Por omisión, la activación automática de Internet Lock está desconectada. Es decir, el bloqueo de Internet sólo puede ser conectado o desconectado manualmente con el botón de Stop situado en el módulo de control. Si quiere conectar las funciones para la activación automática de Internet Lock, active la opción *Enable* dentro del área *Automatic Lock*.



Las opciones para la activación automática de Internet Lock.

3. Una vez conectada la activación automática de Internet Lock, hay dos posibilidades para activar el bloqueo de Internet. Con la opción *Engage Internet lock after X minutes of inactivity*, el bloqueo de Internet se inicia automáticamente tras un periodo determinado de inactividad en el PC. Esta inactividad no se refiere únicamente al tráfico de datos, sino a cualquier tipo de movimiento (similar a lo que ocurre con un salvapantallas). Llevado a cabo de esta forma el bloqueo de Internet, podrá volver a cancelarlo recurriendo expresamente al botón Stop del módulo de control central.

4. Una alternativa similar la ofrece la opción *Engage Internet Lock when screen saver activates*, que acopla la activación del bloqueo de Internet al salvapantallas del PC configurado para todo el sistema. El resultado es parecido, aunque hay algunas diferencias. Por una parte, se puede controlar a nivel central el periodo de inactividad deseado (y probablemente no se produzcan desviaciones entre el salvapantallas y el bloqueo de Internet). De este modo, podremos confiar plenamente que aún estando siempre activado el salvapantallas, el tráfico de datos quedará bloqueado. No obstante, existen salvapantallas que pueden ser ejecutados manualmente cuando se requiere, con lo que también se activaría enseguida Internet Lock. Por lo tanto, existe otra diferencia importante: al desactivar el salvapantallas, también quedará cancelado automáticamente el bloqueo de Internet.

5. Cuando Internet-Lock está activado, hay dos modos de operación de distinta seguridad. Con la opción *Pass Lock programs may access the Internet*, usted permite eludir el bloqueo de Internet a los programas que tengan activada la regla "pass-lock". Con *High Security, All Internet Activity* stopped por el contrario, podrá optar por la forma más segura e impedir cualquier actividad sin importar las demás reglas de aplicación.

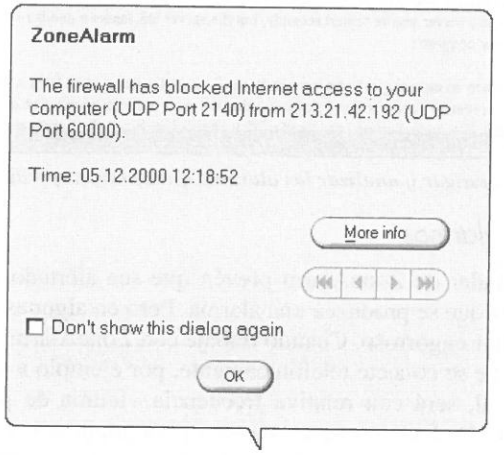
TRUCO

Eludir el bloqueo de Internet con propiedad

En algunos casos, puede resultar conveniente permitir que se eluda el bloqueo de Internet. Si, por ejemplo, tiene configurado su programa de correo electrónico para que a intervalos regulares de 10 minutos compruebe si hay nuevos e-mails, esta configuración sólo podrá funcionar si no se encuentra activo ningún Internet Lock o si el programa de correo electrónico puede eludir el bloqueo. Por lo tanto, habría que activar la regla pass-lock para el programa de correo electrónico (y sólo para éste) y dejar que el bloqueo automático de Internet se ejecute en el modo *Pass Lock Programs may access the internet*, que es menos seguro. Por otra parte, podríamos sostener el criterio de que una comprobación regular del correo electrónico sería innecesaria si Internet-Lock fue activado a raíz de una prolongada inactividad del PC, por lo que usted de todos modos no estaría delante del ordenador. Visto así, el programa podría retrasar tranquilamente la siguiente comprobación, hasta que se volviera a utilizar el PC. En el ámbito general, recomendamos utilizar ZoneAlarm siempre con las configuraciones más seguras posibles, permitiendo excepciones sólo cuando sean estrictamente necesarias y parezcan justificables.

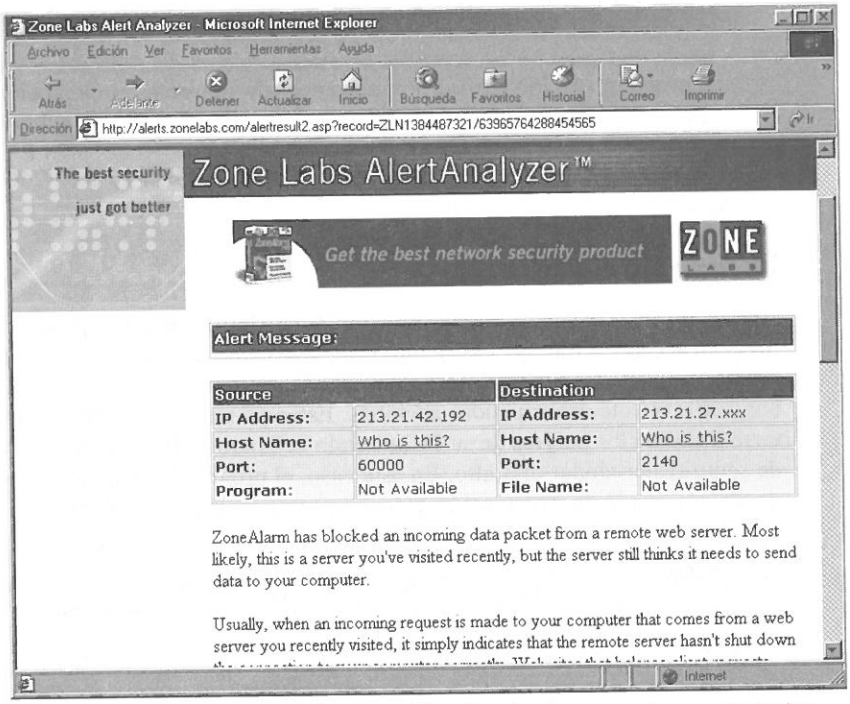
El manejo de alarmas

Aparte de las consultas interactivas de ZoneAlarm, cuando las aplicaciones intentan acceder a Internet existe otro tipo de respuesta posible por parte del programa. Las citadas alarmas se desencadenan siempre que ZoneAlarm impide automáticamente determinadas acciones. Éstas podrían ser el intento de conectarse a uno de los puertos de su PC, estando activado en la zona Internet el nivel de seguridad estándar más alto. En este caso, el programa visualiza una ventana de alarma que le da información esencial acerca de la acción bloqueada.



ZoneAlarm le alerta a usted de un acceso bloqueado.

En la mayoría de los casos, dentro de esta ventana de alarma podrá disponer del botón *More info*, que le permitirá solicitar información adicional acerca de la "avería". ZoneAlarm abrirá el navegador web y desplegará información detallada sobre esa alarma, como por ejemplo qué dirección IP causó la disfunción. Además, el programa facilita ayudas para averiguar la identidad del atacante (*Who is this?*). Por último, aquí encontrará explicaciones sobre lo que significa la alarma exactamente además de sugerencias sobre cómo resolverla. *AlertAnalyzer* es un servicio online del fabricante de Zonealarm, que sólo funciona si su PC está conectado a Internet en ese momento.



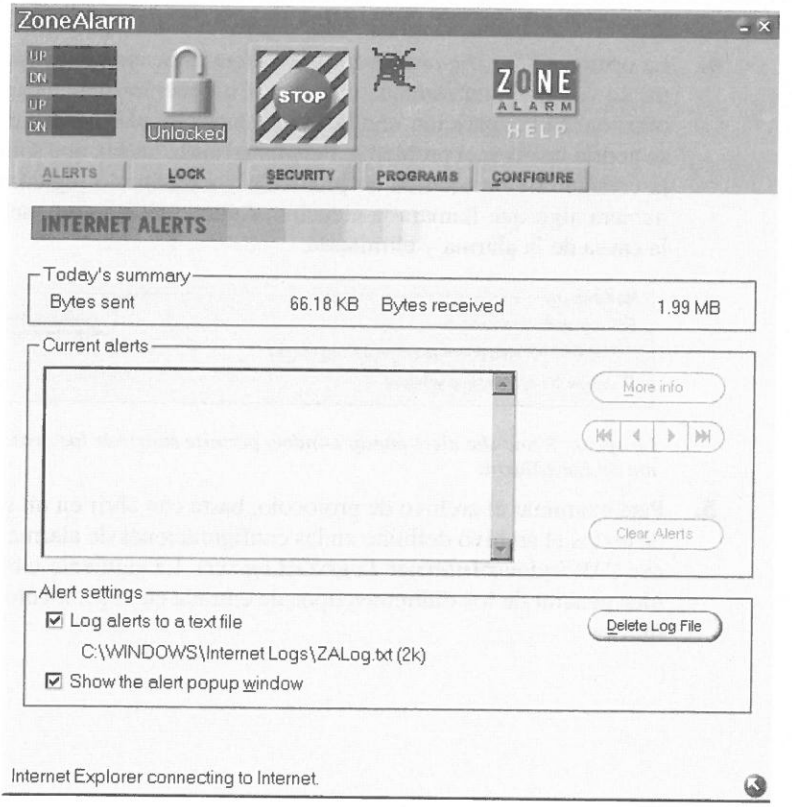
Con AlertAnalyzer, puede investigar y analizar las alarmas que se hayan producido.

Control eficaz de las alarmas

Las configuraciones estándar de ZoneAlarm prevén que sea alertado con una ventana de aviso cada vez que se produzca una alarma. Pero en algunas circunstancias, esto podría resultar engorroso. Cuando trabaje con ZoneAlarm, advertirá pronto que cada vez que se conecte telefónicamente, por ejemplo a través de un proveedor Call-by-Call, será con relativa frecuencia víctima de portscans (vea también el Capítulo 1). Esto no tiene mayor importancia por sí mismo, siempre que los agresores no encuentren un puerto abierto o incluso un troyano

activo. Pero como ZoneAlarm suele desencadenar una alarma a raíz de estos portscans, el asunto podría llegar a ser cargante. De todas formas, existe la posibilidad de encauzar, hasta cierto punto, el comportamiento exacto de ZoneAlarm ante las alarmas.

1. Para ajustar las configuraciones de alarma de ZoneAlarm, dentro del módulo de control central haga clic sobre el botón *Alerts*. Esto llamará a un menú donde podrá encontrar las opciones correspondientes.

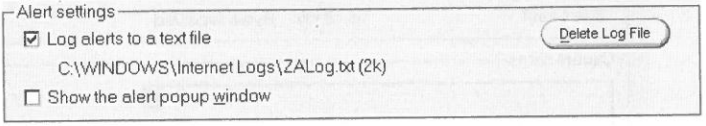


Las configuraciones de alarma de ZoneAlarm.

2. En la parte superior encontrará, en primer lugar, un breve resumen del día (*Today's summary*), con la cantidad de datos enviados y recibidos. Debajo de éste, verá las alarmas actuales registradas por ZoneAlarm. Usando las teclas de desplazamiento, podrá recorrerlas y analizarlas. También aquí, el botón *More info* activa el AlertAnalyzer para la alarma visualizada en ese momento. Con *Clear Alerts*, podrá borrar todas las alarmas visualizadas.

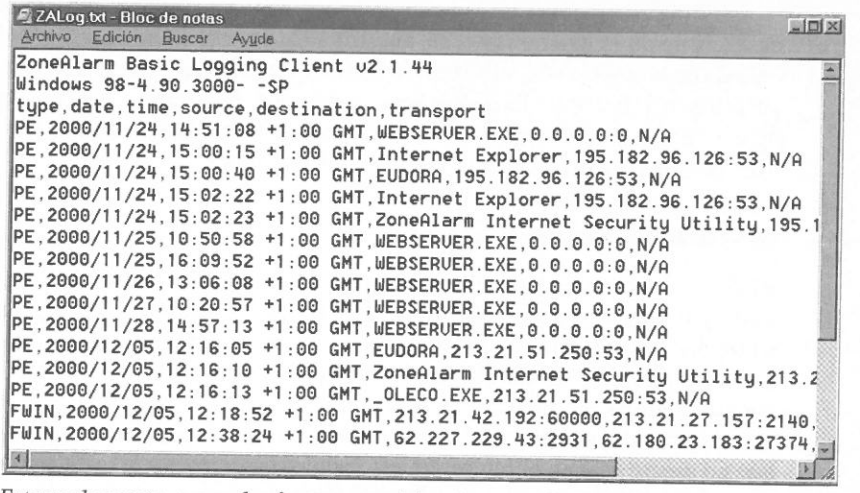
3. Finalmente, en la parte inferior aparecen los *Alert settings*, las configuraciones de alarma. Con la opción *Log alerts to a text file*, conseguirá que todas las alarmas sean protocoladas a un archivo de texto. Debajo, aparecen el nombre exacto y la ruta de ese archivo. Haciendo clic sobre *Delete Log File*, se borrará el contenido actual del archivo y el registro comenzará desde el principio. Siempre resulta conveniente protocolizar las alarmas. Por ejemplo, analizando los datos registrados se pueden reconocer pautas de ataque, o comprobar si de determinadas direcciones ya partieron de ataques en el pasado.

4. La opción *Show the alert popup window* se ocupa de que para cada alarma se visualice una ventana de aviso. Esta opción suele estar activada por omisión. Si la aparición regular de ventanas de alarma llegara a molestar, se podría resolver el problema. Pero en tal caso, habría que solicitar sin falta la creación de un archivo de protocolo y examinarlo regularmente, por si hubiera algo que llamara la atención. Aunque siempre es mejor investigar la causa de la alarma y eliminarla.



La opción Show the alert popup window permite suprimir las ventanas de alarma de ZoneAlarm.

5. Para examinar el archivo de protocolo, basta con abrir en un sencillo editor de textos el archivo definido en las configuraciones de alarma (como estándar *C:\Windows\Internet Logs\ZALog.txt*). La siguiente tabla nos da una idea general de los diferentes tipos de entrada en el protocolo y lo que significan.



Este es el aspecto que suele ofrecer un archivo de protocolo de ZoneAlarm.

Tipo de entrada	Significado	Información que contiene
FWIN	Se bloqueó una consulta entrante	Fecha y hora Dirección IP y número de puerto del ordenador remitente Dirección IP y número de puerto del ordenador destinatario Protocolo empleado (TCP, UDP, ICMP o IGMP)
FWOUT	Se bloqueó una consulta saliente	Fecha y hora Aplicación causante Dirección IP y número de puerto del ordenador destinatario Protocolo empleado (TCP, UDP, ICMP oder IGMP)
PE	Se bloqueó el intento de conexión de una aplicación	Fecha y hora Aplicación causante Dirección IP y número de puerto del ordenador destinatario

Flexible y potente: eSafe para usuarios avanzados

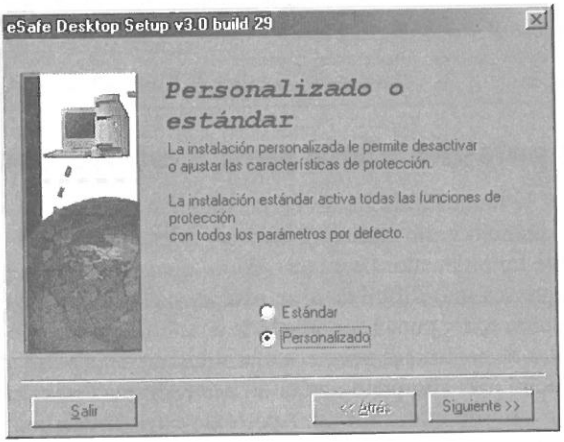
Con *ZoneAlarm* le hemos presentado en las páginas precedentes una solución firewall de fácil manejo y, sin embargo, muy completa, que puede vigilar y proteger eficazmente un ordenador personal. Ahora, queremos mostrarle otra alternativa que, aunque sea más difícil de usar, ofrece en contrapartida mucho mejor rendimiento y, sobre todo, puede ser adaptada de un modo flexible a las necesidades individuales de seguridad. *eSafe* es una solución de seguridad, cuyo planteamiento es mucho más completo que el de ZoneAlarm. También es – aunque no únicamente – una solución firewall. Aparte de esto, ofrece una eficaz administración de usuario mucho más eficiente que la solución de Windows, una protección segura para el test de programas desconocidos, así como un componen-

te antivirus completo. En resumen, estamos ante un paquete que nos permite despreocuparnos enteramente de nuestro PC, ya esté bien desconectado bien online. En este apartado, nos concentraremos en la instalación de eSafe y la preparación del firewall. Para finalizar, queremos dar unas nociones sobre las demás funciones y les remitiremos a otros apartados de este libro, donde también nos ocupamos de eSafe y sus distintas funciones.

Instalar y activar eSafe

eSafe está disponible bajo licencia freeware gratuita y se puede descargar en la dirección http://www.ealladin.com/esafe. De la instalación se encarga un asistente, que en una primera parte le guiará por los pasos habituales (acuerdo de licencia, índice de instalación, etc.). Después viene la parte "interesante", donde nos ocuparemos del espectro de funciones concreto del programa, que ya puede ser definido durante la instalación. Es decir, aquí ya podrá suprimir las partes que no piense usar en el futuro. En este punto, pasaremos a la instalación, donde le mostraremos en qué consisten las diferentes secciones y cuáles son prescindibles o imprescindibles.

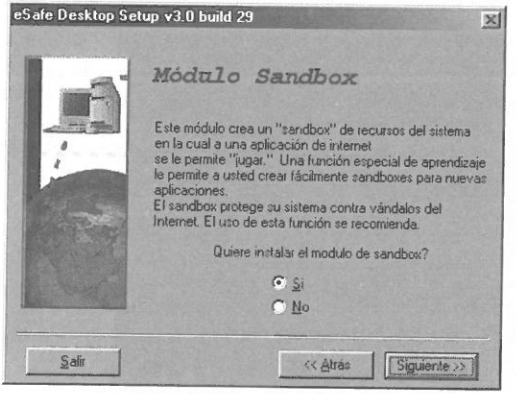
1. El apartado crítico de la instalación comienza con la pregunta de si eSafe debe ser instalado de manera *personalizada* o *estándar*. Le recomendamos encarecidamente la instalación personalizada, ya que podrá decidir individualmente lo que desee instalar. Si ya tiene instalado un software de seguridad, como puede ser un antivirus, debería abstenerse de instalar determinados componentes de eSafe para evitar conflictos. El modo *Estándar* se limita a instalar eSafe íntegro, cosa que resulta recomendable si aún no tiene ningún otro software de seguridad ejecutándose en el PC.



Elija la instalación personalizada para poder configurar óptimamente eSafe.

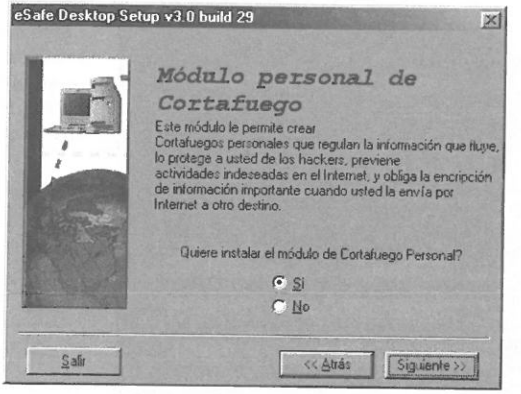
2. En primer lugar, disponemos del módulo *Sandbox*. Se trata de una función

que permite restringir individualmente los permisos de acceso de los programas a los recursos del ordenador. Resulta especialmente indicada para el test de programas nuevos, a los que así se pueden poner restricciones eficaces, con lo que queda reducido el riesgo inherente al test. En un caso normal, este módulo debería ser instalado siempre.



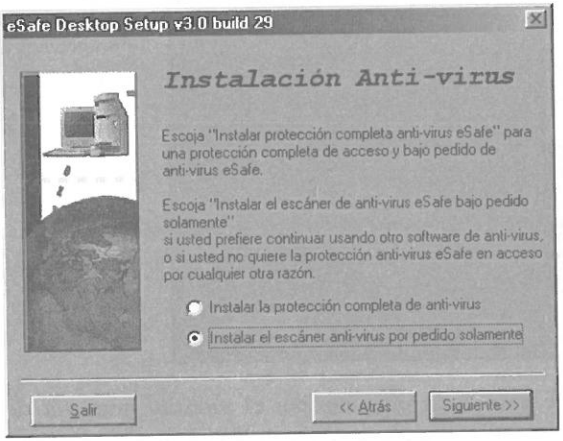
El módulo Sandbox puede poner unos límites eficaces a programas desconocidos o peligrosos.

3. El siguiente paso es la pregunta por el *módulo personal de Cortafuego* (Desktop Firewall), que contiene la verdadera función firewall de eSafe. Si instala el programa, sobre todo, por esta función, obviamente debería seleccionar aquí *Sí*. La cosa cambiaría si ya emplea un programa firewall eficaz con resultados satisfactorios o si su PC está integrado en una red local, con lo que ya lo protegería un buen firewall de hardware. En tal caso, podría renunciar a este módulo de eSafe.



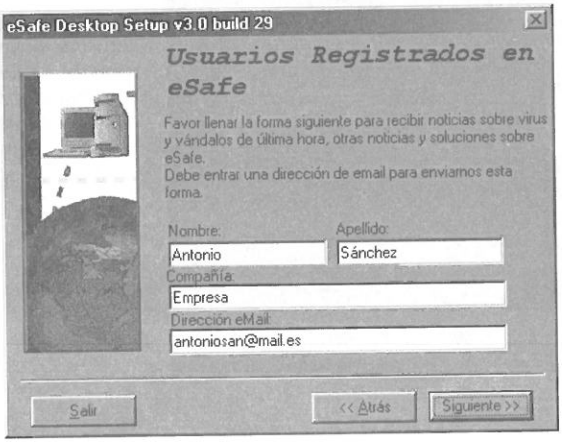
En caso de no tener aún ningún Firewall, debería instalar el módulo de Cortafuego Personal.

4. Finalmente, el asistente le preguntará por la *Instalación de Anti-virus*, el componente de protección antivirus de eSafe. Si aún no es poseedor de un software antivirus, debería instalar el de eSafe íntegramente. De lo contrario, sería conveniente optar por *Instalar el escáner Anti-virus por pedido solamente*. De esta forma, lo tendrá a su disposición cuando lo necesite y, en caso de duda, lo podrá utilizar para un segundo diagnóstico.



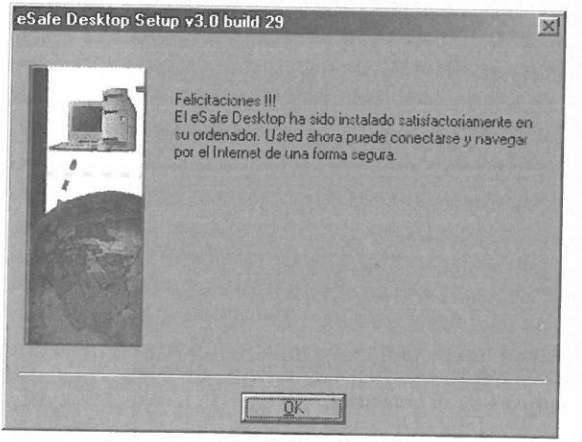
Sólo debería instalar la protección antivirus íntegra si aún no dispone de un software de este tipo.

5. Para concluir, se le pedirá el nombre y la dirección de correo electrónico, datos con los que será registrado en la base de datos de usuarios de eSafe. En el futuro, le mantendrán al corriente, por correo electrónico, de las últimas novedades, aunque también tendrá que contar con recibir algún que otro e-mail publicitario.



Como usuario registrado de eSafe, le mantendrán al corriente por correo electrónico.

6. Con esto concluye la instalación. Aunque, para que eSafe pueda activarse, tendrá que reiniciar el ordenador.



La instalación de eSafe ha concluido correctamente.

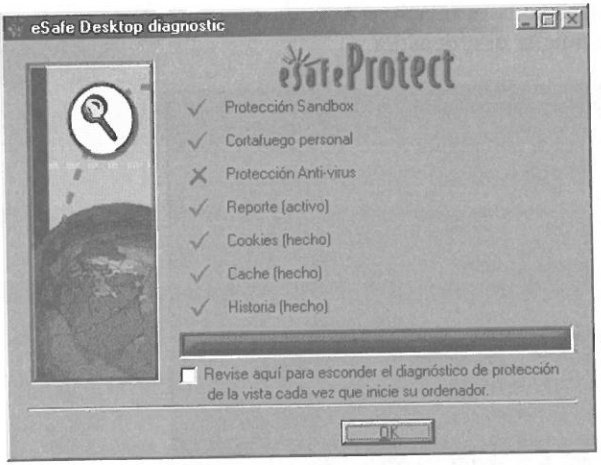
El primer arranque

Tras reiniciar el ordenador, se producirá la primera activación de eSafe. El asistente de configuración verificará si su ordenador tiene programas de comunicación y sus puntos débiles potenciales. eSafe ya reconoce de origen muchos programas de amplia difusión, como los populares navegadores Internet Explorer y Netscape Navigator, pero también otros programas conocidos de Internet como Eudora o el software de acceso de AOL (America On Line). Para estos programas, eSafe dispone de conjuntos de reglas que deciden a qué recursos del sistema puede acceder el software. Naturalmente, usted podrá adaptar esas reglas a sus necesidades particulares, e incluso crear conjuntos de reglas completamente nuevos para los programas que eSafe aún no conozca.

TRUCO

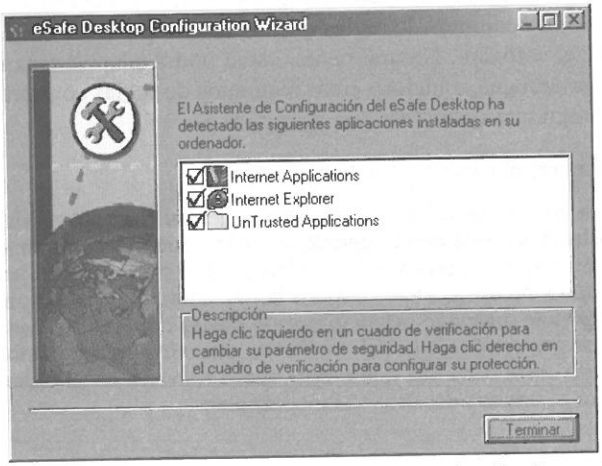
Iniciar manualmente el análisis del sistema

Por definición, eSafe realiza en cada arranque del sistema un análisis del software existente. De este modo, detecta y verifica automáticamente los programas de reciente incorporación. Sin embargo, este procedimiento consume bastante tiempo y no es necesario a todas horas. Usted lo podrá impedir si durante el siguiente arranque activa la opción *Revise aquí para esconder el diagnóstico de protección de la vista cada vez que inicie su ordenador.* Aunque en este caso, cada vez que instale nuevo software en su ordenador, debería iniciar el análisis del sistema manualmente.



eSafe analiza el software de su ordenador.

Una vez concluido el análisis, eSafe le mostrará todos los programas conocidos que haya detectado. A partir de ahora, podrá decidir qué programa debe ser vigilado. Por defecto, la casilla de cada opción ya está activada. Si, por cualquier circunstancia, necesita excluir de la comprobación un software concreto, desactive la casilla de la opción correspondiente. Aunque, normalmente, esto no suele ser necesario. Sólo debería desconectar la comprobación si hay problemas con el programa y está seguro de que puede ser ejecutado sin consecuencias negativas. En el Capítulo 3 profundizamos en el tema del sandbox y en la vigilancia y restricción de aplicaciones.



eSafe notifica todas las aplicaciones de comunicación detectadas.

eSafe en funcionamiento: icono en la barra de inicio y monitor de seguridad

Durante el funcionamiento normal del ordenador, el único indicio de eSafe será un pequeño icono en la parte inferior derecha de la barra de inicio. Adoptando diferentes formas, le avisará del estado de seguridad de su ordenador:

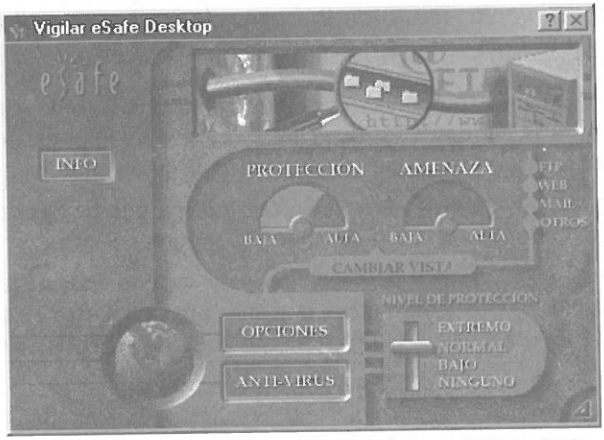
- Un globo terráqueo con rayos descendentes significa, que eSafe está activo y funciona con normalidad. Su ordenador está seguro.
- Un globo terráqueo con rayos descendentes parpadeando, indica igualmente que hay protección. Además, ahora hay una conexión activa en su ordenador, lo cual significa mayor peligro. No obstante, su ordenador está seguro.
- Un globo terráqueo con rayos rojos significa alerta máxima. eSafe no está activo (puede que haya sido desactivado temporalmente) y en este momento, el ordenador se encuentra desprotegido.

El símbolo del globo terráqueo indica en todo momento el estado de seguridad de eSafe.

Haciendo doble clic sobre el icono, abrirá el monitor de seguridad, que le dará una información más detallada sobre el estado del sistema.

- La escala *Protección* reproduce el nivel de seguridad de su sistema. Ésta depende del *Protection Level* (nivel de protección) que usted eligiera.
- El indicador *Amenaza* le revelará la intensidad de la actividad desarrollada en ese momento en su ordenador relevante para la seguridad. Ésta depende, por ejemplo, de las conexiones online existentes y de las aplicaciones que fueran iniciadas.
- A la derecha verá los indicadores de las distintas actividades online, que se dividen en *FTP* (transferencia de archivos), *WEB* para la Red, *MAIL* para el correo electrónico y *OTROS*.
- Debajo del monitor, podrá ajustar el nivel de protección. Dispone de cuatro niveles: *NINGUNO* (ninguna seguridad), *BAJO*, *NORMAL* y *EXTREMO* (seguridad muy alta). Normalmente, la opción *NORMAL* ofrece un buen término medio entre seguridad y rendimiento. *EXTREMO* sólo es necesario para aplicaciones muy críticas. *NINGUNO* es una configuración que, a ser posible, no debería ser indicada nunca en eSafe. Sólo es conviene hacerlo, si una aplicación requerida urgentemente es entorpecida en extremo.

Asimismo, el monitor de seguridad permite acceder directamente al asistente de configuración (*OPCIONES*) y al *ANTI-VIRUS*.

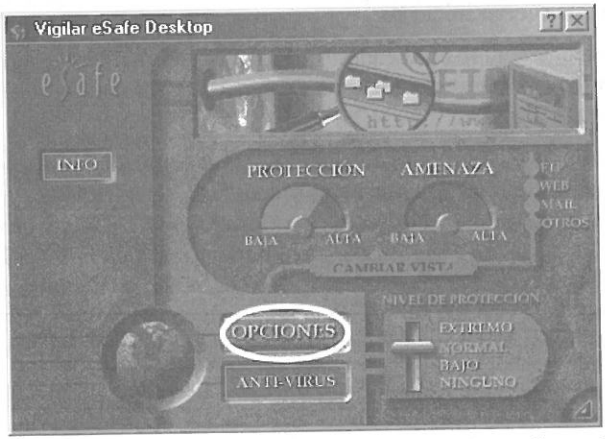


Todo de un vistazo: el monitor central de seguridad de eSafe.

Emplear eSafe como un firewall

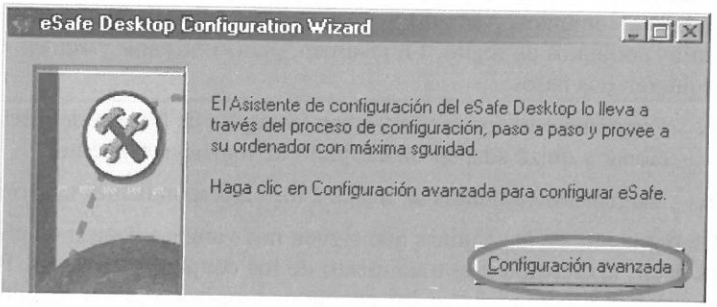
Una vez instalado y activado eSafe, usted podrá dedicarse a preparar el módulo firewall. Muy importante: al contrario de otros productos, nada más concluir la instalación eSafe no brinda ninguna protección. Sólo cuando el filtro haya sido configurado correctamente, se activará el firewall. eSafe ofrece una amplia gama de posibilidades para definir reglas destinadas al firewall. A continuación, les mostramos las configuraciones más importantes.

1. Encontrará el acceso a las configuraciones de firewall (y todas las demás opciones del programa) en el monitor de seguridad de eSafe. Dentro de éste, haga clic sobre el botón *OPCIONES*.



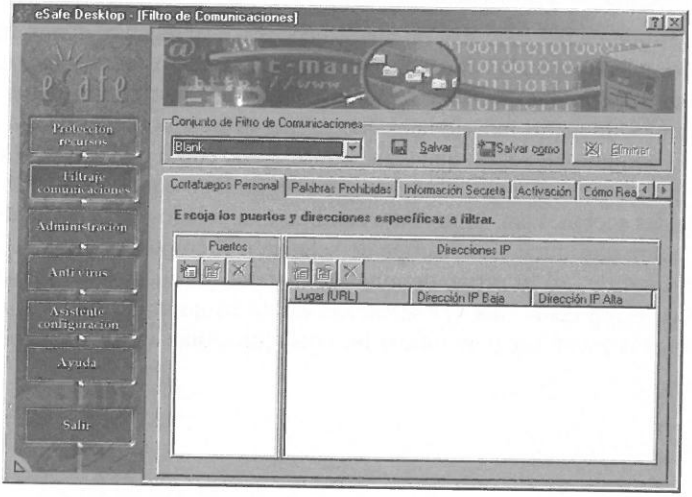
Mediante el botón OPCIONES tendrá acceso a las configuraciones de eSafe.

2. Con esto, primero activará el asistente de configuración, que le permite configurar eSafe paso a paso. Pero para emprender las configuraciones individuales del firewall, lo mejor es hacer clic sobre el botón *Configuración avanzada*.



La configuración avanzada le conducirá directamente a las configuraciones individuales.

3. Este botón le conducirá directamente a los extensos menús de configuración de eSafe. Con la barra de desplazamiento, situada en el margen izquierdo de la ventana, podrá cambiar entre las diferentes categorías de las opciones. Aquí, se visualiza la categoría más alta de *Sandbox* o *Protección de recursos*. Para acceder a la configuración del firewall, haga clic sobre el botón *Filtraje de comunicaciones* de la barra de navegación. Esto hará que aparezcan en la mitad derecha de la ventana las pestañas y opciones necesarias para configurar el firewall.



Las opciones del firewall de eSafe.

Emplear conjuntos de reglas predefinidos

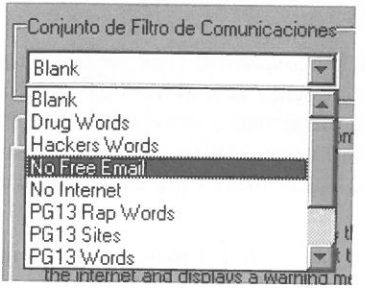
Uno de los conceptos básicos de eSafe son los conjuntos de reglas. Como la flexibilidad de las configuraciones de eSafe permite crear multitud de reglas, resulta difícil manejarlas una a una. Por eso, las reglas ya definidas pueden ser agrupadas en conjuntos. Así, en lugar de reglas sueltas, se asigna al usuario uno o varios conjuntos de reglas. En resumen, para configurar y activar el firewall se requieren dos pasos:

1. Crear uno o varios conjuntos con las reglas de filtrado del firewall, o seleccionar y quizá adaptar un conjunto de reglas ya existente.
2. Asignar los conjuntos de reglas a los correspondientes usuarios.

De momento, en las páginas que siguen nos vamos a centrar en el primer paso, es decir, la creación y el tratamiento de los conjuntos de reglas. Para concluir, mostraremos cómo asignar los conjuntos terminados a los diferentes usuarios. Antes de empezar a crear o modificar reglas de filtrado, es recomendable familiarizarse con el manejo de los conjuntos de reglas, ya que suponen la única posibilidad de guardar permanentemente las modificaciones realizadas. Encontrará las funciones para gestionar los conjuntos de reglas dentro de las configuraciones de firewall o cortafuegos, en la parte superior del área *Conjuntos de protección de recursos.*

Las funciones para gestionar los conjuntos de reglas.

A la izquierda del todo hay un cuadro de lista desplegable, donde figuran todos los conjuntos de reglas almacenados en eSafe. Entre estos hay tanto una serie de reglas predefinidas que fueron grabadas durante la instalación, como también los conjuntos de reglas individuales que se fueran creando y guardando con el tiempo. El conjunto de reglas que viene configurado como estándar es *Blank* (vacío), que prácticamente no contiene ninguna regla. Esto equivale a decir que permite todas las acciones sin límite. Para cambiar a uno de los otros conjuntos de reglas, basta con introducir en el campo de selección el conjunto deseado. Vigile que al seleccionarlo, no lo active de ninguna manera, ya que sólo lo llama para trabajar con él, es decir, una vez seleccionado un conjunto de reglas, en los diferentes menús podrá ver y modificar las configuraciones desglosadas.



Con el campo de lista desplegable se le permite elegir los conjuntos de reglas con los que quiera trabajar.

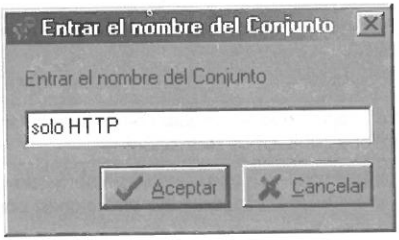
Durante la instalación de eSafe ya se implantaron una serie de conjuntos de reglas predefinidos, que pueden ser fácilmente aprovechables. Al mismo tiempo, estos conjuntos pueden servir de ejemplo y propuesta para la creación de reglas propias. La siguiente tabla proporciona una idea general de los conjuntos de reglas predefinidos y lo que significa cada uno.

Nombre del conjunto de reglas	Significado
Blank	El conjunto de reglas "vacío" que se emplea como estándar tras la instalación. ¡No contiene NINGUNA restricción!
Drug Words	Un filtro de palabras que contiene (unas pocas) palabras clave sobre el tema "Drogas" y criba las correspondientes direcciones, páginas web y/o grupos de noticias.
Hackers Words	Un filtro de palabras que incluye una extensa lista con palabras clave sobre el tema "Hacker", que criba las correspondientes direcciones, páginas web y grupos de noticias.
No Free Email	Un filtro de palabras que contiene numerosas expresiones y direcciones del ámbito "Correo electrónico gratuito" y filtra las correspondientes direcciones, páginas web o grupos de noticias.
No Internet	Un filtro de puertos muy restrictivo, que impide eficazmente todo tráfico con Internet.
PG13 Rap Words *PG13 Sites* *PG13 Words*	Tres filtros de protección de menores, que todos juntos se encargan de filtrar las direcciones y palabras clave inapropiadas para niños y adolescentes.
Racist Words	Filtro de palabras que reúne una extensa recopilación de expresiones racistas internacionales.
Spanish Profanity	Una recopilación de palabrotas españolas que son suprimidas mediante un filtro de palabras.
Trojan/Hackers Ports	Un filtro de puertos que bloquea el tráfico de datos en todos los puertos que suelen ser empleados por troyanos o herramientas de hackers similares.

Definir conjuntos de reglas propios

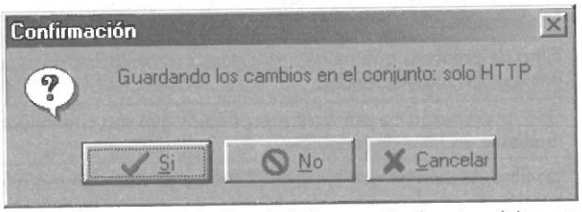
Aparte de los conjuntos de reglas predefinidos, también es posible crear todos los conjuntos propios que se deseen. Un conjunto de reglas propio se basa, siempre, en uno ya existente. Si alguno de los predefinidos se aproxima bastante a las reglas que usted necesite establecer, podrá aprovecharlo y adaptarlo a sus necesidades. Si no, emplee simplemente el conjunto *Blank* que no contiene ninguna regla.

Una vez haya creado sus propias reglas dentro de los menús (en las siguientes páginas le explicaremos cómo hacerlo), guárdelas como un conjunto de reglas propio, haciendo clic sobre el botón *Salvar como* en el área *Conjuntos de protección* de recursos. A continuación, aparecerá la ventana de entrada *Entrar el nombre del conjunto*, donde deberá teclear el nombre del nuevo conjunto de reglas. Le recomendamos emplear una denominación que exprese, con la mayor exactitud posible, la función que desempeñe ese conjunto. Sólo así podrá encontrarlo después con rapidez y seguridad en una lista más extensa. Confirme los datos introducidos con *Aceptar*.



Ponga a sus conjuntos de reglas nombres adecuados.

Si, más adelante, necesita realizar cambios en un conjunto de reglas ya definido, bastará con hacer clic sobre el botón *Salvar*. No hará falta volver a introducir cada vez el nombre del conjunto. Si tras haber modificado el conjunto seleccionado quiere salir de la configuración de firewall o cambiar a otro conjunto de reglas sin haber grabado antes las modificaciones, eSafe se lo advertirá mediante un aviso. Aquí se le sugerirá guardar los cambios, desecharlos o cancelar todo el proceso y regresar a las configuraciones iniciales de ese conjunto de reglas.



Ningún cambio se pierde. eSafe le recordará automáticamente que guarde las modificaciones.

Definir filtros de puerto propios

En la categoría *Cortafuegos personal* de la configuración de firewall (*Filtraje de comunicaciones*), eSafe ofrece la posibilidad de definir reglas propias de filtrado de puertos. Este filtrado de determinados puertos, según reglas previamente definidas, es una de las funciones básicas de un firewall. Permite bloquear los diferentes servicios de Internet a nivel general, o sólo para ciertos usuarios. En el siguiente ejemplo, queremos mostrarle cómo controlar mediante un filtro de puerto el acceso de un PC a los grupos de noticias. Para ello, formulamos una regla que bloquee toda comunicación en el *News-Port 119* estándar, a excepción de un servidor de noticias muy concreto.

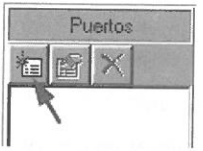
INFO

TCP/IP y puertos

En el protocolo de Internet TCP/IP, la comunicación va subdividida en diferentes capas o niveles. A fin de cuentas, lo que se pretende es que en un vínculo de red puedan ejecutarse en paralelo varios servicios de Internet. Por ejemplo, se quieren recibir y enviar correos electrónicos y al mismo tiempo, navegar por la Red. Para permitir esta utilización paralela de varios protocolos, la comunicación va organizada en puertos. Esto podría compararse con una autopista de diferentes carriles. Hay una serie de puertos estándar para los servicios fundamentales de Internet (por ejemplo el Puerto 80 para el servidor web). Aparte de este, se dispone de varios miles de puertos libres que pueden ser utilizados a voluntad. Un firewall es capaz de bloquear determinados puertos y así, desactivar totalmente los correspondientes servicios para un ordenador.

En la dirección http://www.isi.edu/in-notes/iana/assignments/port-numbers se puede encontrar una lista muy completa de las ocupaciones de puertos actualmente vigentes.

1. Para definir un filtro de puerto, en primer lugar debe seleccionar los puertos donde tenga que actuar el filtro. Para ello, haga clic sobre el botón *Nuevo puerto*, situado dentro del área *Puertos*.



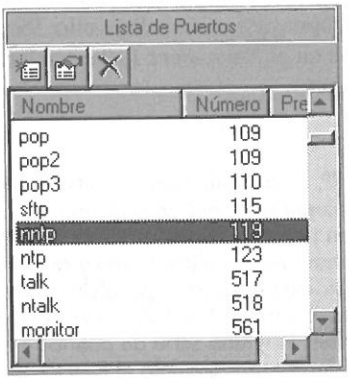
Cree primero un nuevo puerto.

2. Ahora, podrá seleccionar el puerto deseado en la lista de puertos situada a la derecha. Aquí figuran todos los puertos conocidos por el programa, con su nombre y número. Para nuestro ejemplo, seleccionamos el puerto *NNTP* 119, que representa al *Network News Transport Protocol* NNTP, responsable del intercambio de datos a través de grupos de noticias.

TRUCO

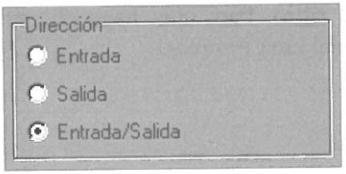
Añadir más puertos

eSafe presenta en la lista de puertos sólo aquellos que conoce. Pero usted puede introducir manualmente todos los puertos que desee, con un simple clic sobre el botón *Añadir nuevo puerto*, situado en la parte superior izquierda. Aparecerá una ventana adicional donde podrá introducir el nuevo puerto (por ejemplo el puerto "ICQ" con el número 4000), que a partir de ese momento también figurará en la lista de puertos.



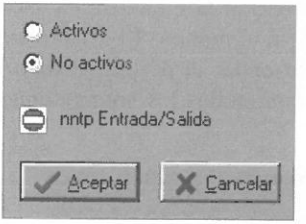
Seleccione en la lista de puertos el que desee filtrar.

3. Una vez establecido el puerto a filtrar, deberá indicar en qué dirección quiere que se filtren los datos de ese puerto. Se pueden filtrar sólo los datos de *entrada* (desde otros ordenadores a su PC), sólo los de *salida* (desde su PC a otros ordenadores), o los datos de *entrada/salida*. En el ejemplo, queremos definir como estándar la paralización completa del tráfico de noticias, por lo que nos decidimos por la opción *Entrada/Salida*.



¿En qué dirección hay que filtrar los datos en tránsito?

4. Finalmente, habrá que indicar si queremos que el tráfico de datos para el puerto elegido y la dirección seleccionada sea activado (*Activo*) o desactivado (*No activos*).



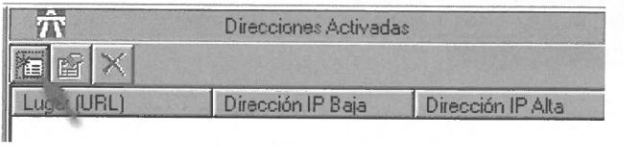
El puerto seleccionado puede ser activado o desactivado por norma.

5. Debajo de esta opción, hay un práctico resumen abreviado de las configuraciones actuales. El símbolo indica si la configuración estándar del puerto es activada (símbolo de autopista verde-blanco) o desactivada (símbolo rojo de "cerrado al tráfico"). Le sigue el nombre del puerto y la dirección de filtrado. Con un clic en *OK* se guarda el filtro de puerto elegido de este modo.

6. De vuelta en el menú de comunicaciones, encontrará en el área *Ports* una entrada para el filtro de puerto recién creado. En nuestro ejemplo, hemos generado un filtro que bloquee todo tráfico de datos a través del puerto NNTP y así evite con eficacia cualquier intercambio de noticias.

El filtro de puerto para NNTP ha sido creado.

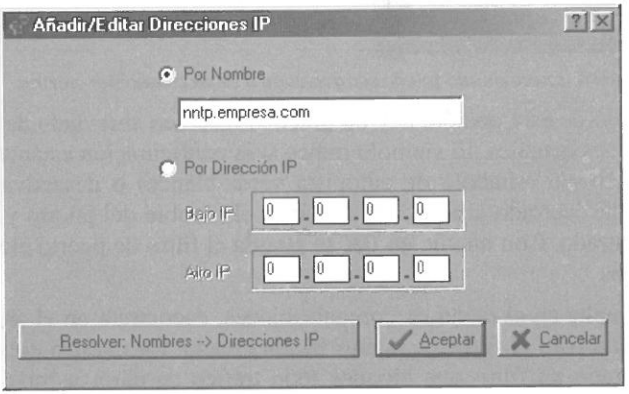
7. Sin embargo, en nuestro ejemplo queríamos permitir el intercambio de noticias con un servidor de noticias muy concreto, que nos parece inofensivo. Ahora debemos formular en el área *Direcciones Activadas* una excepción a la regla de filtrado. Eso se logra haciendo clic sobre el botón *Nueva dirección*, situado en la parte superior izquierda de esa sección.



Para hacer excepciones a las reglas, hay que indicar las direcciones permitidas.

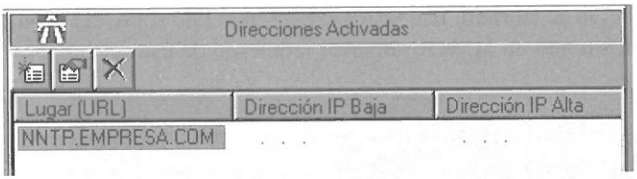
8. Aparece la ventana *Añadir/Editar Direcciones IP*. Aquí podrá indicar el nombre IP del ordenador (en este ejemplo, el servidor de noticias), con el que deberá permitirse el intercambio de datos a pesar del filtro de puerto. Seleccione la opción *Por Nombre* y en el campo inmediatamente inferior, indique el nombre completo del ordenador. Como alternativa, también

podrá seleccionar la opción *Por Dirección IP* e indicar, en los campos inferiores correspondientes a esta opción, el número IP del ordenador. Esto es muy interesante, porque permite extender el permiso excepcional a toda una gama de ordenadores, por ejemplo todos los ordenadores de la propia empresa.



Indique el nombre IP o el número IP de las direcciones permitidas.

9. Una vez introducida de una manera u otra la dirección IP, guarde la excepción haciendo clic sobre *OK*. Esto le devolverá a la sección *Cortafuegos personal*, donde encontrará la nueva entrada en el campo *Direcciones Activadas*. Siguiendo el modo descrito, usted puede definir para cada filtro de puerto tantas direcciones excepcionales como quiera. Tan sólo tendrá que tener en cuenta que la excepción generada únicamente será válida para el filtro de puerto que hubiera seleccionado en el área *Puertos*. No afectará a los demás filtros de puerto del mismo conjunto de reglas.



La excepción a la regla figura en la lista de direcciones permitidas.

Con esto, ya ha creado un filtro de puerto completo. Pero tenga en cuenta que no será activado hasta que lo guarde dentro de un conjunto de reglas y lo asigne a un usuario. Cuando este usuario (y con él, también el conjunto de reglas) esté en activo, eSafe verificará todos los paquetes de datos que entren en ese puerto, aceptando sólo los que vengan de los ordenadores definidos como excepción. Los contenidos de todos los demás paquetes ni siquiera llegarán a su ordenador, por lo que tampoco podrán causarle daños.

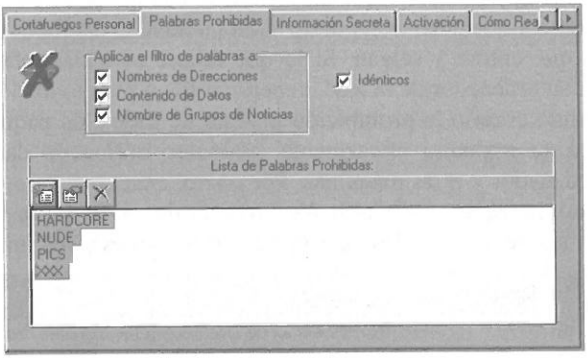
Con este procedimiento, podrá generar filtros para otros puertos como Telnet, TFP, SMTP o POP. Por ejemplo, es conveniente dejar activados sólo aquellos puertos que realmente desee utilizar. Supongamos que no quiere emplear la aplicación de mensajes ICQ y no quiere que nadie más la use desde su PC. En ese caso, puede bloquear completamente el puerto habitual de ICQ (el 4000) para los paquetes de datos que entren y salgan. Si lo que quiere es aislar totalmente, durante un tiempo, su ordenador de la Red, genere un filtro para todos los puertos y seleccione como criterio la prohibición general de todos los paquetes de entrada y salida. Esto impedirá eficazmente cualquier tráfico de datos por TCP/IP entre su ordenador y otras máquinas. Por cierto, exactamente esto es lo que hace el conjunto de reglas predefinido *No Internet* de eSafe. En la siguiente tabla, se muestra una relación de los puertos más importantes y sus funciones.

Número de puerto	Nombre de puerto	Significado
20 + 21	FTP	Transferencia de archivos (File Transfer Protocol)
23	Telnet	Control remoto por Telnet
25	SMTP	Protocolo de salida de correo (Simple Mail Transfer Protocol)
80	HTTP	Transferencia de páginas web (Hypertext Transfer Protocol)
109-110	POP	Protocolo de entrada de correo (Post Office Protocol – POP o POP3)
119	NNTP	Transferencia de grupos de noticias (Network News Protocol)
529	IRC	Internet Relay Chat

Filtrar los paquetes de datos por su contenido

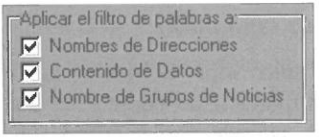
Los filtros de puerto clásicos trabajan "sólo" sobre la base de las informaciones de dirección, es decir, analizan la información de control de los paquetes de datos para averiguar de dónde vienen, adónde van y cómo son; filtrándolos según las reglas guardadas. No les interesa el contenido en sí, es decir, si es peligroso o no. De esta forma, puede ocurrir que en algunos casos se excedan mientras que en otros dejen pasar contenidos absolutamente cuestionables, por la sencilla razón de que no se creó el filtro de puerto adecuado. Por ello, como complemento a los filtros de puerto, eSafe busca un segundo planteamiento basado en el contenido, recomponiendo temporalmente todos los paquetes que entran y salen para poder verificar su contenido. De este modo, eSafe puede bloquear transferencias de datos que contengan determinadas palabras clave. Evidentemente, esta función resulta muy indicada para cuestiones de protección de la infancia y del menor, cribando por ejemplo páginas web o correos electrónicos con determinados conceptos inmorales. Pero también puede servir para proteger eficazmente la información confidencial, según verá a continuación.

En la categoría *Palabras prohibidas*, puede mantener una lista con palabras clave cuya aparición haga que eSafe bloquee la correspondiente página web, dirección o noticia.



eSafe puede filtrar y bloquear los contenidos con palabras clave indeseables.

1. Si usted quiere crear una lista con palabras clave prohibidas, decida primero qué clase de información deberá ser explorada en busca de estas palabras clave. Para ello, active las opciones correspondientes en el apartado *Aplicar el filtro de palabras a:*. *Nombres de direcciones* impide la transmisión de cualquier dirección de ordenador (también direcciones web) que incluya alguna de las palabras clave. *Contenido de datos* explora el propio contenido de todos los paquetes de datos transmitidos y Nombre de grupos de noticias filtra los *nombres de grupos de noticias* introducidos en busca de palabras vetadas.



El campo de acción del filtro de contenido puede ser definido con suma exactitud.

2. Adicionalmente, usted puede indicar si habrá que exigir una concordancia exacta (*Idénticos*) en la exploración de direcciones y contenidos. En este caso, el filtro sólo encontraría algo si el término de búsqueda figura como expresión aislada. Por ejemplo, si emplea como término clave "Porno", sería filtrada la dirección *www.porno.com*, pero no *www.pornografia.com*. Si por el contrario desactiva la concordancia exacta, serían filtradas las dos direcciones. Esto último quizá sea lo más conveniente para la protección de niños y menores.

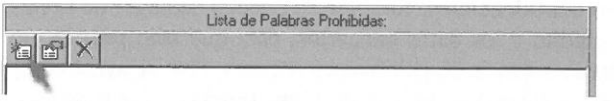
En la mayoría de los casos, la concordancia exacta no resulta recomendable.

INFO

¿Cuándo interviene el filtro de palabras clave?

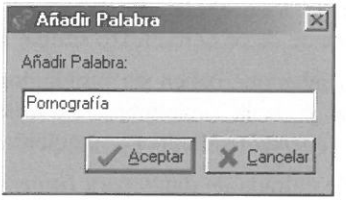
Para emplear eficazmente el filtro de palabras clave, debería tener claro cómo funciona. Tomemos "Sex" como ejemplo. Si usted activa la exploración de direcciones (*Nombres de direcciones*) en busca de esta palabra, toda dirección que contenga la expresión "Sex" (como por ejemplo *www.sex.com* o *www.sex-world.com*) será cribada. Es decir, cuando alguien pida una página de esa dirección, será rechazado de plano. Así, aunque esta página quizá no contenga la expresión prohibida, jamás llegará al ordenador. En los *nombres de grupos de noticias*, el procedimiento es similar. Cuando eSafe explora el contenido de los paquetes de datos, filtra exactamente aquellos paquetes que contengan el concepto clave problemático. Como una página web es transmitida en multitud de paquetes de datos, la página no tendría por qué ser bloqueada completamente. En función de su estructura, quizá sólo le faltaran determinadas partes (inmorales). Aunque en la mayoría de los casos, cabe esperar el bloqueo completo de la página web. Una advertencia más: eSafe sólo es capaz de verificar el contenido si éste viene incluido directamente en los paquetes de datos. En soportes de información indirectos como por ejemplo imágenes, el filtro no puede funcionar. Es decir, "pornografía" como concepto clave no bastaría para filtrar también imágenes pornográficas.

3. Finalmente, introduzca en el apartado *Lista de palabras prohibidas* las palabras clave que deban desencadenar el bloqueo de la correspondiente página web o dirección. Por desgracia, aquí no se pueden teclear simplemente los conceptos o tomarlos de otro archivo. En lugar de eso, hay que teclearlos uno a uno en un diálogo de entrada. Para ello, haga clic sobre el botón *Añadir*, situado en la parte superior izquierda de este apartado.



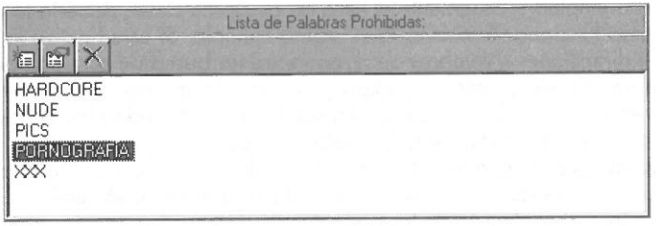
Haga clic sobre el botón Añadir, para incluir en la lista las palabras clave nuevas.

4. En la ventana siguiente (*Añadir palabra*), teclee el concepto que quiera incluir en la lista de palabras prohibidas. Debe introducir la palabra tal y como deberá ser filtrada. Si hay varias formas de escribirla, lo mejor será que cree varias entradas (por ejemplo: Pornografía – Pornographie). Guarde la entrada haciendo clic sobre *Aceptar*.



Introduzca el concepto que quiera incluir en la lista como concepto clave.

5. A continuación, verá la nueva entrada en la lista de palabras prohibidas.



Los nuevos conceptos clave son incluidos en la lista de palabras prohibidas.

6. Para concluir, le recomendamos guardar en un conjunto de reglas propio la lista de conceptos clave generada de este modo. Así, quedarán grabados y podrán ser asignados después a determinados usuarios.

Proteger datos confidenciales mediante el filtro de contenido

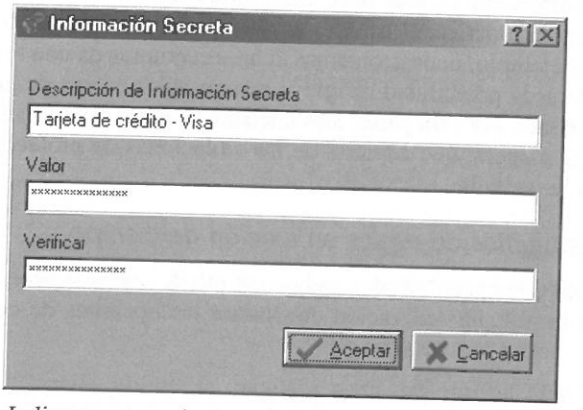
El protector de eSafe para *Información secreta* trabaja según el mismo planteamiento que la lista de palabras prohibidas. En principio, no es otra cosa que una lista de información confidencial, que le protege a usted de enviar accidentalmente por Internet datos secretos sin encriptar. Si, por ejemplo, quiere evitar que alguien con quien tenga contacto a través de Internet averigüe su número de teléfono particular, podrá incluirlo en la lista de información secreta. eSafe verificará el contenido de todos los paquetes que salgan y lo comparará con esa lista. Si por algún descuido, su número de teléfono se hubiera colado en un correo electrónico o en un documento enviado, eSafe bloqueará la transmisión y protegerá así sus datos confidenciales. También se pueden proteger de la misma forma las tarjetas de crédito y los datos bancarios, para que sólo puedan enviarse encriptados, es decir, a través de conexiones seguras. Así, si usted compra en tiendas virtuales, no tendrá que preocuparse. Si una tienda quiere transmitir sus datos sin encriptar, eSafe intervendrá inmediatamente e impedirá la transferencia.

Esta función también le puede proteger de los caballos de Troya que quizá colara algún hacker en su ordenador (vea el Capítulo 3). Si uno de estos programas espía intenta enviar a su autor por Internet las contraseñas hurtadas u otros datos confidenciales, eSafe los interceptará, siempre que estuvieran incluidos en la lista de información secreta. Por supuesto, podrá seguir enviando, como de costumbre, los datos confidenciales encriptados. eSafe sólo intercepta las palabras clave si están incluidas en un paquete de datos como texto simple sin encriptar.

1. Para definir los datos confidenciales que deben ser protegidos, entre en la categoría *Información Secreta* y, en la *Descripción de datos sensibles*, haga clic sobre el botón *Nueva entrada* situado a la izquierda del todo.

2. Ahora, se abrirá una ventana de entrada de datos para *Información secreta*, donde podrá definir cada vez una información confidencial.

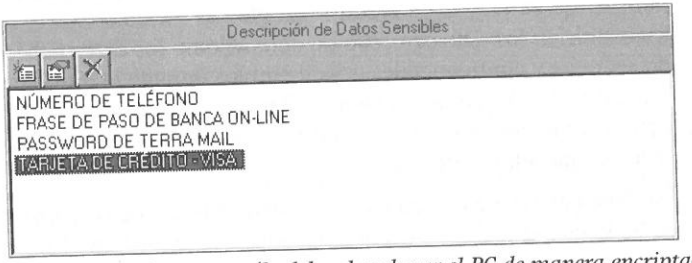
3. En primer lugar, introduzca una *Descripción de información secreta*. Esta descripción sólo es para su propia orientación y la puede omitir si quiere. No tiene otra finalidad que dejar lo más claro posible de qué datos se trata.
4. Debajo de ésta, indique en *Valor* la información a proteger, por ejemplo el número de su tarjeta de crédito. Emplee el formato exacto con el que se transmitirían los datos en caso de duda. Como los datos deben seguir siendo secretos y confidenciales, eSafe emplea durante la introducción una técnica similar a la que se usa para teclear contraseñas, es decir, en lugar de los caracteres reales, sólo podrán verse asteriscos. Así, se pretende proteger los datos de miradas curiosas.
5. Para asegurarse de que ha tecleado realmente los datos correctos (como no se ve lo que se teclea), vuelva a introducir lo mismo en el campo *Verificar*.
6. Si después usted hace clic sobre *Aceptar*, eSafe verificará si las dos entradas coinciden exactamente. De no concordar, el programa reaccionará y le pedirá la corrección.



Indique con exactitud los datos que eSafe deba proteger si son revelados accidentalmente.

7. Si lo que había introducido era correcto, será aceptado y se generará una entrada nueva en la lista de datos confidenciales. En ésta, sólo verá la descripción que usted hizo anteriormente para esa entrada.
8. Asimismo, es posible modificar una entrada ya creada – por ejemplo, si ha habido cambios en su cuenta bancaria o en el número de la tarjeta de crédito –, señalando la entrada en la lista y haciendo clic sobre el botón del centro *Cambiar o modificar entrada*. De esta manera, volverá a abrir la ventana de *Información secreta* ya conocida, donde tendrá oportunidad de cambiar todos los campos de entrada.

9. Si ya no necesita una entrada, también la puede borrar. Márquela en la lista y haga clic sobre el botón *Borrar entrada* definido con una pequeña cruz roja. Atención: ¡La entrada será borrada inmediatamente, sin petición de confirmación!



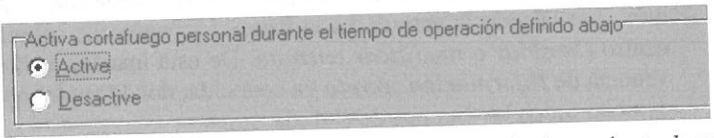
La información secreta sólo debe abandonar el PC de manera encriptada.

eSafe protege toda la información que haya sido definida aquí, recurriendo al mecanismo del filtro de contenido. Los paquetes de datos que incluyan alguna información confidencial de este tipo, serán bloqueados y no podrán abandonar el ordenador. En la práctica, el usuario se dará cuenta de esto por los mensajes de error. Si, por ejemplo, tiene problemas al hacer compras en una tienda virtual, debería considerar la posibilidad de que la responsable sea una de las funciones protectoras de eSafe. Por otra parte, más adelante le enseñaremos a configurar el programa de tal manera, que advierta de las violaciones de protección sacando un mensaje en la pantalla.

Activar los conjuntos de reglas en función del tiempo

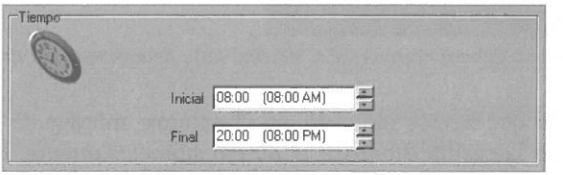
Se puede definir con exactitud para cada conjunto de reglas si debe ser activado y cuándo. En la pestaña Activación encontrará las opciones de configuración necesarias.

1. Aquí podrá definir, en primer lugar, si quiere *Activar* (Active) o *Desactivar* (Desactive) el conjunto de reglas recién seleccionado. Esto se traduce en la ventaja de que no hace falta borrar enseguida un conjunto de reglas que no sea necesario de momento. En su lugar, basta con desactivarlo para, más adelante, volver a activarlo cuando se requiera. Tenga en cuenta, que esta configuración sólo se refiere al conjunto de reglas seleccionado, no a todo el firewall como tal. Si para el usuario activo rigen más conjuntos de reglas, estos podrán seguir activos a pesar de todo.



Esta configuración permite activar o desactivar cualquier conjunto de reglas.

2. Un poco más abajo, podrá indicar un periodo de tiempo durante el cual deberá estar vigente la activación o desactivación seleccionada anteriormente. Supongamos que usted quiere evitar que durante el día, alguien aproveche su ausencia para navegar por Internet. En tal caso, genere un conjunto de reglas que bloquee todos los puertos (o recurra al conjunto de reglas predefinido *No Internet*) y actívelo, por ejemplo, de 8.00 de la mañana a 20.00 de la tarde. Durante ese tiempo, eSafe no permitirá ningún tráfico de datos en ningún puerto, con lo que el acceso a Internet quedará bloqueado con fiabilidad. Así, podrá evitar que quizá otros miembros de la familia naveguen desde su PC sin que usted lo sepa y lo infecten con virus o troyanos.

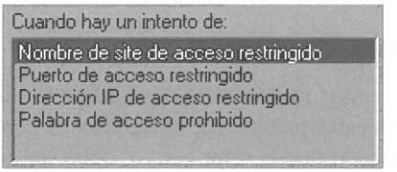


Los conjuntos de reglas pueden ser activados o desactivados automáticamente para un periodo de tiempo determinado.

Reacciones a violaciones de las reglas

Finalmente, debe comunicar a eSafe cómo tiene que reaccionar en caso de una violación de protección; es decir, si hay un intento de transmitir datos a los que afecte una regla determinada. Para ello, dispone de varias posibilidades en la categoría *Reacción*.

1. Seleccione primero en el apartado *Cuando hay un intento de* la acción para la que desee definir una reacción. eSafe distingue varias configuraciones para accesos ilícitos a páginas web, puertos, direcciones IP y palabras prohibidas.

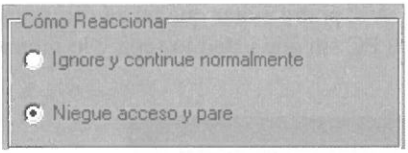


Seleccione en primer lugar el tipo de acción para la que desee definir una reacción.

2. Ahora, en el recuadro *Cómo reaccionar* podrá elegir para la acción seleccionada a la izquierda, una de las dos reacciones posibles. *Ignore y continúe normalmente* es la elección menos recomendable. Si se encuentra activada esta opción, eSafe ignorará la regla de filtrado y, pese a la infrac-

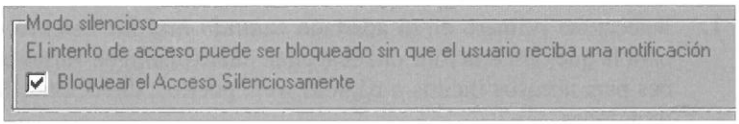
ción cometida, proseguirá con la acción iniciada por el usuario. Por regla general, esto no tiene sentido. Por lo tanto, la reacción estándar a todas las acciones es *Niegue acceso y pare*. Aquí, eSafe interrumpirá rigurosamente la acción que desencadenó el filtro.

3. Defina la reacción apropiada para toda clase de acciones ilícitas o verifique si la reacción estándar *Niegue acceso y pare* ha sido realmente definida para todas las acciones.



Seleccione cómo deberá reaccionar el sistema ante determinadas infracciones de la regla.

4. Aparte de lo que hemos indicado, en el extremo inferior de esta sección podrá activar la casilla *Bloquear el acceso silenciosamente*. Ésta suprime todo tipo de ventanas de advertencia y avisos por parte de eSafe. En su lugar, registra en un archivo de protocolo todas las acciones censurables y las reacciones del sistema. Este modo resulta especialmente indicado si usted quiere emplear eSafe para restringir y vigilar a otros usuarios de su PC. Dichos usuarios no advertirán que están siendo controlados por eSafe, sólo que determinadas direcciones o páginas web a veces no pueden ser solicitadas. Sin embargo, usted podrá comprobar posteriormente en el protocolo, si los otros usuarios han desencadenado alguna regla de filtrado.



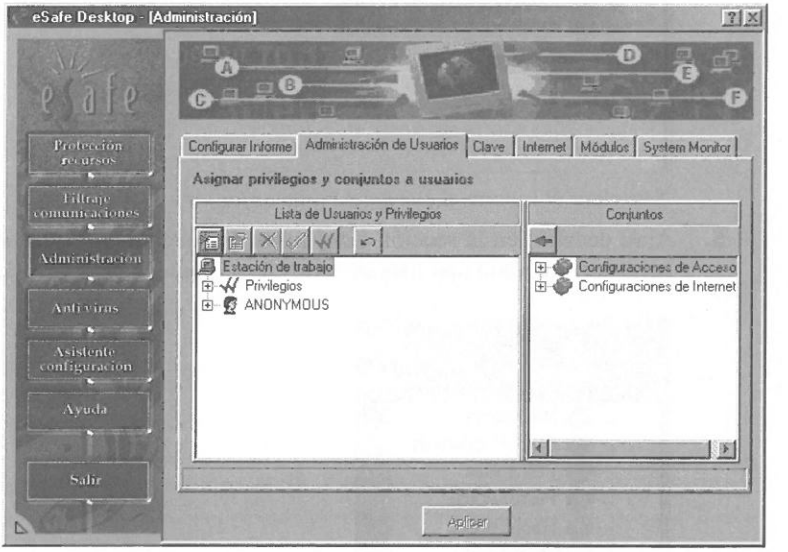
El modo de aviso permite vigilar bajo cuerda a otros usuarios del PC.

Asignar conjuntos de reglas a los usuarios

En las páginas precedentes le hemos mostrado las posibilidades de eSafe para definir reglas de filtrado y cómo éstas pueden ser agrupadas en conjuntos. Para que un conjunto de reglas terminado pueda estar activo, debe ser asignado a un usuario. Para ello, deberá seleccionar los usuarios en el administrador de usuarios de eSafe y asignarles los conjuntos de reglas definidos anteriormente. En el Capítulo 2, ya presentamos con más detalle el administrador de usuarios de Windows y el de eSafe. Por lo que aquí nos vamos a limitar a exponer los pasos básicos para asignar conjuntos de reglas.

1. Para poder asignar un conjunto de reglas a un usuario, tendrá que entrar en las configuraciones de eSafe. En la ventana de configuración, pulse sobre el botón *Administración* para ir a esa sección.

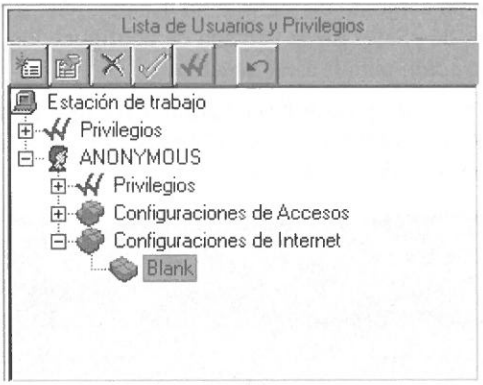
2. Aquí, también las pestañas y opciones de administración se subdividen en varias categorías. Abra la categoría *Administración de usuarios* para acceder a las configuraciones de usuarios de eSafe.



En el Administrador de Usuarios de eSafe puede establecer con exactitud los derechos de cada usuario.

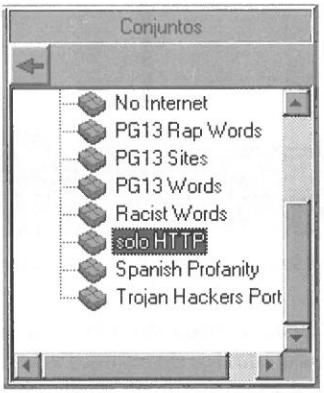
3. Ahora, seleccione en el apartado Lista de usuarios y privilegios, el usuario a quien quiera asignar uno o varios conjuntos de reglas. En la lista verá una entrada para cada usuario que quizá se introdujo en su día. Si aún no había empleado la administración de usuarios de eSafe, debería seleccionar el usuario Anónimo (*Anonymous*), cuyos derechos recibirán todos los usuarios para los que no se creara expresamente una entrada propia. (Si desea más información sobre la administración de usuarios de eSafe, puede consultar el Capítulo 2).

4. Abra para el usuario seleccionado la subentrada *Configuraciones de Internet*. Aquí verá los conjuntos de reglas válidos hasta la fecha para ese usuario. Generalmente, sólo tiene el conjunto de reglas vacío (*Blank*).



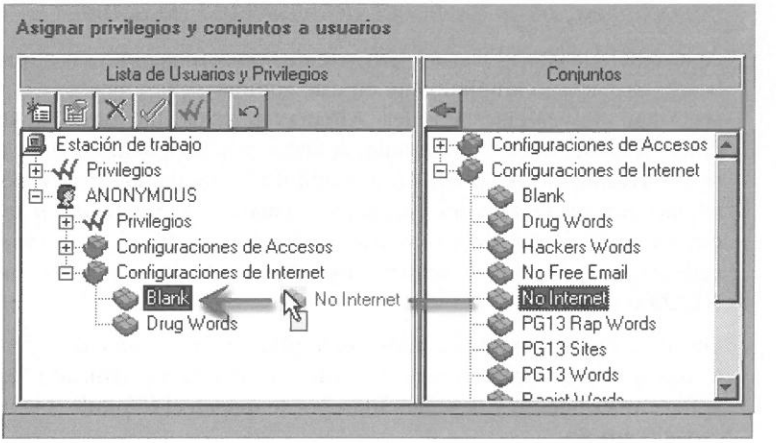
Seleccione el usuario al que quiera asignar los conjuntos de reglas.

5. Abra después en la sección *Conjuntos*, la subentrada *Configuraciones de Internet*. Recibirá una lista de todos los conjuntos de reglas definidos.



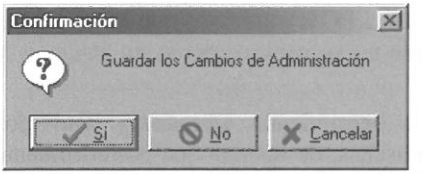
Bajo Configuraciones de Internet encontrará todos los conjuntos de reglas definidos.

6. Si para el usuario seleccionado a la izquierda quiere aprovechar uno de los conjuntos de reglas existentes, marque ese conjunto en la derecha y después, haga clic en *Asignar*.Alternativamente, también puede "seleccionar" el conjunto de reglas con el puntero del mouse y, manteniendo la tecla izquierda del ratón pulsada, "arrastrarlo" hacia la zona izquierda y soltarlo sobre el usuario. En ambos casos, el efecto es el mismo: el conjunto de reglas será asignado a ese usuario y a partir de entonces, aparecerá en la subentrada de *Configuraciones de Internet*.



Asigne los conjuntos de reglas que se muestran en la zona derecha al usuario seleccionado en el lado izquierdo.

7. De este modo, podrá asignar a un usuario todos los conjuntos de reglas ya existentes que desee. Una vez asignados a ese usuario (y a todos los demás, según el caso) todos los conjuntos que necesite, tendrá que guardar las modificaciones. Esto es muy fácil. Basta con trasladarse dentro de la barra de desplazamiento a uno de los otros apartados, o hacer clic en el botón *Salir* para cerrar la ventana de configuración. eSafe le consultará si quiere guardar las modificaciones realizadas mediante el cuadro de diálogo *Confirmación*. Confirme la consulta con el botón *Sí*. Si, por el contrario, no las quiere guardar, podrá desecharlas con *No* o cancelar todo el proceso con *Cancelar*.



Guarde las modificaciones que hiciera en las propiedades del usuario.

Según se ha descrito a fondo en el apartado sobre la Administración de Usuarios del Capítulo 2, eSafe se basa en el administrador de usuarios de Windows. Si se registra en dicho administrador un nuevo usuario, eSafe activará automáticamente los conjuntos de reglas que le fueran asignados a ese usuario. Si usted no hubiera empleado el administrador de usuarios de Windows o si se registra un usuario desconocido, eSafe recurrirá al usuario general o anónimo (*Anonymous*) y empleará las reglas asignadas a éste. Por lo que las reglas para ese usuario especial deberían ser lo más restrictivas posible.

Panorámica: otras funciones de seguridad de eSafe

Aparte del Desktop Firewall (*filtraje de comunicaciones* en el programa) que hemos presentado ampliamente en este capítulo, eSafe posee más funciones de seguridad convenientes y útiles. Algunas de estas funciones las abordamos en otras partes del libro. Por ejemplo, el tema de la administración de usuarios recibe un tratamiento detallado en el Capítulo 2, donde mostramos cómo complementar con eSafe al administrador de usuarios de Windows, más bien insuficiente; para convertirlo en un sistema fiable y eficaz cuya seguridad no tenga nada que envidiar a la de sistemas operativos más profesionales como Windows NT/2000 o UNIX.

Otra función de seguridad sumamente práctica es el sandbox, que permite restringir y vigilar aplicaciones. Resulta especialmente indicado para examinar aplicaciones nuevas y desconocidas, por lo que en el Capítulo 3 le dedicamos un espacio propio.

4.2 La confianza está bien, el control aún mejor – vigilar el ordenador

Los programas presentados hasta ahora en este capítulo, protegen el PC de ataques desde la red o Internet. Pero según hemos demostrado en los capítulos precedentes, los ataques no tienen por qué partir de una red conectada. El propio PC puede servir de herramienta para un ataque si alguien tiene acceso directo a él. Entendemos por acceso directo la posibilidad de entrar en la habitación donde se halla el PC y hacerse furtivamente con acceso al monitor, al teclado y las unidades externas de almacenamiento de datos (especialmente disquetera y CD-ROM). Si lo consigue, un hacker puede:

- Localizar directamente en el PC los archivos que desee y almacenarlos en un disquete, de modo que no necesite perpetrar un ataque a través de una red.
- Extraer del PC, con las herramientas apropiadas, datos confidenciales, como por ejemplo contraseñas, de manera que posteriormente pueda perpetrar un ataque desde la Red sin esforzarse mucho ni levantar revuelo.
- Cambiar discretamente la configuración del PC, para facilitar un ataque posterior.
- Instalar clandestinamente software especial que, por ejemplo, registre los datos introducidos por el usuario (¡espionaje de contraseñas!), o abra una puerta trasera en el sistema para aprovecharla más tarde siempre que quiera (troyano).

Para evitar estos ataques, no deberíamos limitarnos a proteger la conexión de nuestro ordenador a la red, sino también el acceso al propio PC. Naturalmente, la solución más eficaz sería guardar al PC bajo llave mientras no lo usemos. Pero esto casi siempre es imposible, cuando el ordenador es el de la oficina o si compartimos el PC doméstico con otros miembros de la familia. Incluso si tenemos posibilidad de cerrar con llave el ordenador o la puerta de la oficina, la protección sólo será tan eficaz como lo sea el cerrojo. Un hacker que persiga un objetivo serio y sólido, no retrocederá ni ante un robo.

Controlar los ataques y otras actividades

Por lo tanto, si no podemos restringir de una forma fiable el acceso al PC, al menos deberíamos controlar con exactitud lo que ocurre en él cuando no lo empleamos nosotros. La solución más conservadora sería vigilar la habitación por vídeo, pero esto no resulta práctico, ya que es un método relativamente caro, e incluso difícil de aplicar sin que el atacante lo detecte enseguida. Además, una cámara de vigilancia casi nunca puede registrar con exactitud lo que ocurre en la pantalla, ya que el usuario suele sentarse delante de ella. ¡Pese a todo, no habría que desdeñar el valor disuasorio de una cámara de vigilancia o incluso de un simulacro apropiado!

Pero resulta mucho más eficaz usar al propio PC como instrumento de vigilancia. A fin de cuentas, basta con instalar un programa que se ejecute discretamente en segundo plano y registre con exactitud todo lo que ocurra en el PC.

Un programa de este tipo es *Salus*, que se puede descargar en versión de prueba bajo la dirección http://www.ezetest.com/salus. Una vez instalado, Salus se oculta en segundo plano y registra multitud de información:

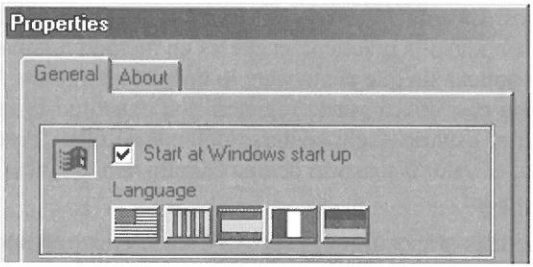
- horarios de arranque y terminación de una sesión en Windows, inclusive el usuario que se registrara,
- el arranque de aplicaciones y la apertura de documentos,
- el establecimiento y la conclusión de enlaces con Internet, como por ejemplo conexiones telefónicas a Internet,
- las direcciones de Internet y páginas web que fueran visitadas y solicitadas,
- los caracteres, las palabras y los textos que introdujera el usuario,
- los datos de texto que fueran intercambiados entre aplicaciones a través del portapapeles.

Cualquiera de estos datos, por sí solo, ya puede ser muy valioso. Pero si se le solicita, el programa puede representarlos todos conjuntamente en una secuencia temporal continua. Así, se obtiene una idea muy exacta de las acciones ejecutadas por un usuario en el PC.

Preparar Salus para la vigilancia

Salus se instala mediante un práctico asistente, que ejecuta automáticamente casi todos los pasos necesarios. Tan sólo deberá realizar unas pocas configuraciones para adaptar el programa a sus necesidades. Por ello, al final de la instalación aparece un menú donde podrá ajustar las configuraciones más importantes.

1. En la zona superior del menú *Properties*, configure primero el comportamiento de arranque de Salus. Como valor por omisión viene activada *la* opción *Start at Windows start up*, es decir, Salus siempre arrancará al mismo tiempo que Windows, lo que parece ciertamente la solución más lógica. Si desactiva esta opción, tendrá que iniciar el programa siempre manualmente.



Seleccione el comportamiento de arranque y los idiomas de la interfaz para Salus.

2. Más abajo, en *Language* podrá elegir el idioma que debe aparecer en la interfaz de Salus. Para hacerlo, basta con que haga clic sobre el botón representado con la bandera correspondiente (esta configuración no es de efecto inmediato, entra en vigor después del primer arranque del programa de administración).

3. Dentro del apartado *Activation* (activación), encontrará el campo *Introduce the text that will make the application visible.* Introduzca aquí la secuencia de caracteres con la que deba ser activado el programa de administración de Salus. La palabra secreta estándar es *trial*, pero no es recomendable conservarla, ya que todos los demás usuarios de Salus también la conocen. Seleccione en su lugar una secuencia de caracteres propia que, a ser posible, debería ser tan característica que nadie la pudiera introducir por casualidad (por ejemplo, al redactar un texto).

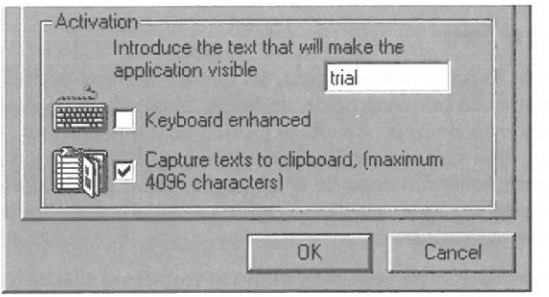
INFO

Activación mediante palabra secreta

Para poder funcionar de verdad, Salus depende de que los usuarios vigilados, ya tengan permiso de acceso o no, no se percaten de que están siendo controlados. Es decir, no deben encontrar el programa de ninguna manera. Por eso, Salus tampoco aparece en estado activo en la barra de tareas ni en

la lista de tareas. Se ejecuta con absoluta discreción en segundo plano. Para activar el programa de administración, introduzca simplemente la secuencia de caracteres que definió cuando hizo las configuraciones. Usted puede teclear estos caracteres secretos dentro de cualquier aplicación, o en cualquier cuadro o diálogo de texto donde se permita una entrada de datos libre. En principio, también se podría poner a teclear dentro del escritorio de Windows, aunque este no proporcione ninguna posibilidad de introducir datos. Salus vigila el teclado y arranca automáticamente el programa de administración en cuanto haya sido introducida la secuencia de caracteres previamente definida. Por lo tanto, debería elegir una secuencia que nunca pueda teclear otro usuario por casualidad, es decir, evite nombres sencillos, combinaciones numéricas puras o similares.

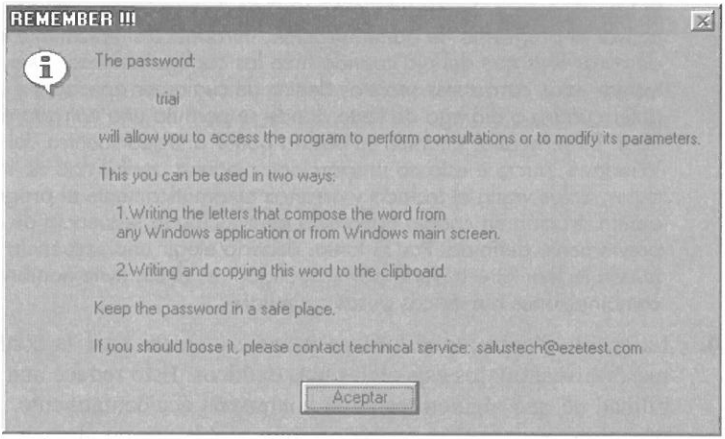
4. La casilla *Keyboard enhanced* permite emplear para la contraseña, además, otros símbolos especiales más exóticos. Esto reduce aún más la posibilidad de que alguien teclee la contraseña accidentalmente. Aunque, por otra parte, esta opción podría originar problemas en algunas aplicaciones, por lo que en caso de duda debería permanecer desactivada.



Introduzca la contraseña con la que deba ser activado el programa de administración de Salus.

5. Finalmente, la opción *Capture texts to clipboard* se encarga de que Salus también registre todos los textos que fueran desplazados al portapapeles tras cortar o copiar. Por norma, aquí el texto almacenado se limita a los primeros 4096 caracteres, para ahorrar espacio en memoria.

6. Guarde las configuraciones seleccionadas con *OK*. Antes de que Salus arranque definitivamente, se muestra una ventana de advertencia donde se le mostrará una vez más la palabra secreta elegida. Incluye, además, instrucciones para arrancar el programa de administración de Salus con ayuda de esta palabra secreta.



La última advertencia, antes de que Salus desaparezca definitivamente a un segundo plano y comience su vigilancia.

TRUCO

La contraseña de Salus

Memorice bien la contraseña elegida, ya que es la única posibilidad de llegar al programa de administración de Salus. Si pierde la contraseña, sólo le quedará el recurso de pedir ayuda al fabricante del programa. Aunque, por regla general, éste sólo ayudará a los usuarios registrados, que son los que pagan religiosamente. En caso de emergencia, usted puede desinstalar el programa desde *Agregar o quitar programas* del panel de control, pero perderá los datos registrados.

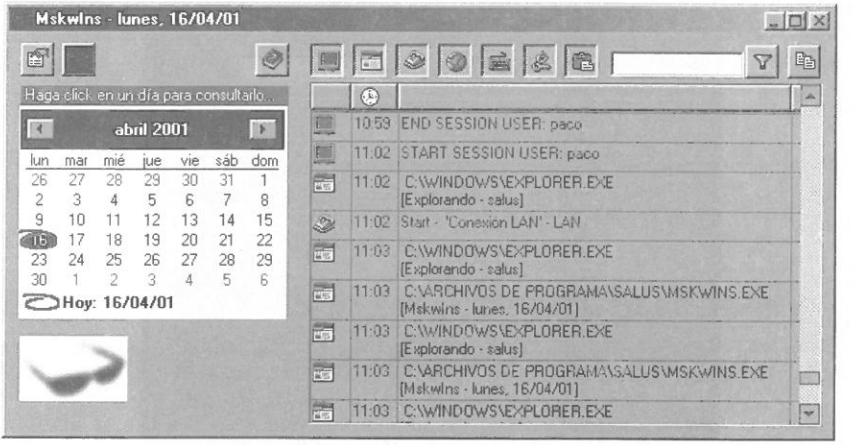
Ahora, Salus estará activo en segundo plano y registrará todos los datos relevantes. Si ya realizó la correspondiente configuración estándar, será activado cada vez que arranque de nuevo el ordenador y registrará eficazmente todo lo que se haga en ese PC.

Analizar los registros de Salus

Si Salus ya estuvo activo en segundo plano, usted podrá llamar en todo momento al programa de administración para analizar los registros. Para tal fin, basta con que introduzca la combinación de caracteres que definiera en las configuraciones. En cuanto haya tecleado el último carácter, arrancará automáticamente el programa de administración. En la versión de prueba gratuita, sólo tendrá que cerrar la ventana de aviso adicional haciendo clic sobre *Continue*.

En la mitad izquierda de la ventana de administración encontrará un calendario, donde podrá elegir el día cuyos registros quiera analizar. En la versión de muestra gratuita sólo queda grabado el día actual, que también es seleccionado automáticamente. Con el botón *Propiedades* situado en el extremo superior izquier-

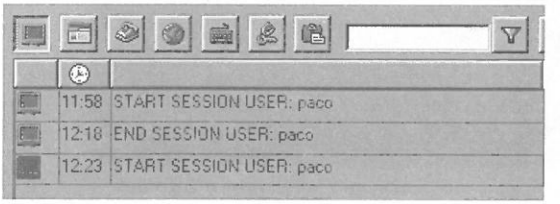
do, podrá mostrar el menú de configuración. Aquí podrá cambiar las configuraciones indicadas inicialmente (por ejemplo, cambiar la palabra secreta). Con el botón *Esconder y continuar* representado con unos ojos de felino, puede hacer desaparecer Salus de nuevo, ejecutándose en segundo plano.



En el programa de administración de Salus vienen registradas todas las acciones por orden cronológico.

En la mitad derecha de la ventana encontrará el protocolo de acciones y todas las funciones relacionadas con él. Los botones situados encima de la lista de acciones son filtros, que permiten conectar y desconectar la aparición de ciertas informaciones. Vamos a presentar, de izquierda a derecha, estos botones y lo que significa cada uno:

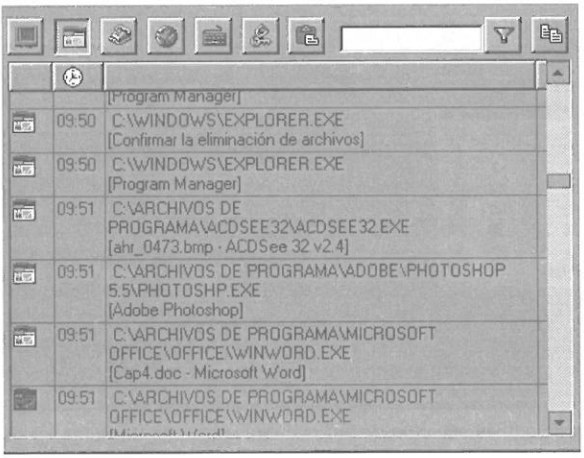
- *Inicio/fin de sesión*: registra cuándo comenzó o finalizó Salus el protocolo de una sesión y qué usuario se dio de alta. Si Salus arranca automáticamente con Windows, el tiempo coincidirá con el comienzo y la finalización de las sesiones y los usuarios de Windows.



Salus revela qué usuario inició o finalizó una sesión y cuándo lo hizo.

- *Ventanas (títulos):* registra todas las ventanas visualizadas en pantalla, quedando así registradas todas las aplicaciones que sean iniciadas. Como la mayoría de las aplicaciones también reflejan en la línea de título de su ven-

tana el nombre del documento recién abierto, Salus casi siempre incluye en el registro el nombre de los documentos que fueran abiertos con las aplicaciones. Cada vez que el usuario se centra en una ventana, el programa generará una entrada. Esto permite hacer un seguimiento muy exacto de las acciones de los usuarios.

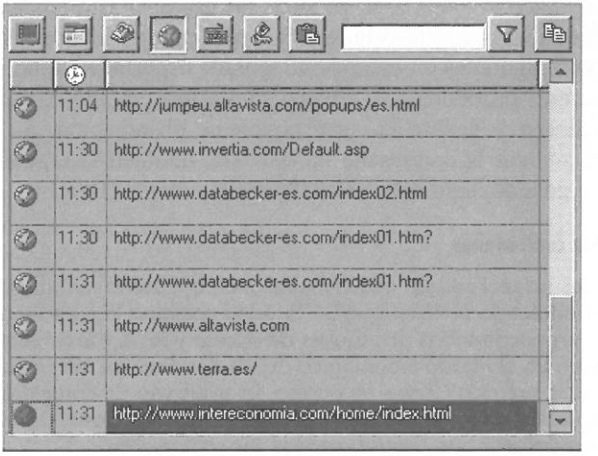


Salus registra todas las aplicaciones iniciadas y los documentos que fueran abiertos con ellas.

- *Inicio/fin de la conexión a Internet:* en cada conexión telefónica, Salus registra el momento de comienzo y de finalización. Además, para el establecimiento de la conexión indica el aparato y el enlace de teletransmisión de datos con los se produjera la toma de contacto.

Salus registra todas las conexiones telefónicas a Internet.

- *Páginas visitadas (WWW):* Salus registra todas las direcciones web que fueran visitadas por los usuarios. Aquí no importa si la dirección fue tecleada directamente, seleccionada desde favoritos o introducida de cualquier otro modo. Para cada llamada, se genera una entrada con la hora.



Salus registra las direcciones de todas las páginas web visitadas.

- *Texto escrito:* Salus registra todos los caracteres introducidos por los usuarios. Para cada texto que fuera introducido de una sola vez, se genera una entrada propia. Si el usuario realizó entremedias alguna otra acción (por ejemplo cambiar a otra aplicación), Salus genera una nueva entrada. El registro es tan preciso, que se puede reproducir con exactitud el proceso de creación de un texto, por poner un ejemplo. También pueden aparecer en la lista otras entradas de datos interesantes, como por ejemplo contraseñas o claves electrónicas.

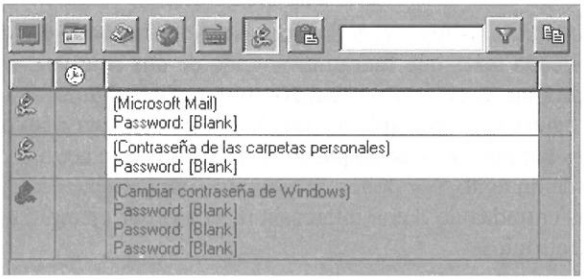
Salus registra todos los datos que el usuario introdujera por teclado.

- *Claves de acceso*: Salus registra todas las acciones para las que el usuario deba introducir una palabra clave. Para ello, aprovecha que las contraseñas suelen ser solicitadas en campos de entrada especiales, donde en lugar de los caracteres introducidos aparecen sólo asteriscos (***). Salus reconoce estos diálogos y genera la correspondiente observación. Si el programa puede reconocer la contraseña introducida, también la registrará. Aunque por regla general, aquí sólo suele figurar la entrada [Blank].

TRUCO

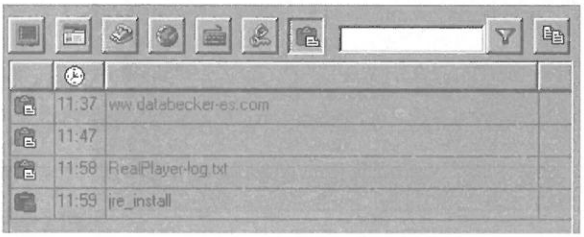
Averiguar contraseñas

Que Salus no reproduzca textualmente una contraseña introducida, no significa que no pueda ser averiguada. Si usted combina las representaciones visuales proporcionadas por *Claves de acceso* y las de *Texto escrito*, a veces, encontrará en el listado cronológico de los dos tipos de información, justo detrás de la entrada *Claves de acceso*, la secuencia de caracteres exacta que introdujo el usuario cuando le fue pedida la palabra clave. De esta forma, puede controlar si otro usuario conoce sus contraseñas.



Salus registra hasta las contraseñas de usuario introducidas.

- *Texto en Portapapeles:* Si Salus ha sido configurado adecuadamente, también genera una entrada cada vez que el usuario traslade algún texto al portapapeles con la función cortar o copiar, para intercambiarlo desde allí con otras aplicaciones. Cada una de estas entradas contiene como máximo los primeros 4096 caracteres del texto. No se guarda más, por razones de espacio.



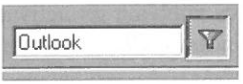
También cuando se trasladan textos al portapapeles, Salus hace un registro.

Los distintos tipos de entradas pueden ser combinados a voluntad. Salus siempre generará aquellas entradas para las que esté activado (o "pulsado") el correspondiente botón en la parte superior, cumpliendo rigurosamente el orden cronológico. Se pueden activar al mismo tiempo varios o incluso todos los botones, con lo que se recibe un protocolo muy exacto de la totalidad de acciones de los usuarios. Así, también existe la posibilidad de relacionar los diferentes tipos de entradas entre sí. Por ejemplo: ¿Qué introdujo un usuario tras haber abierto determinado documento en el procesador de textos?

Buscar en el protocolo de Salus

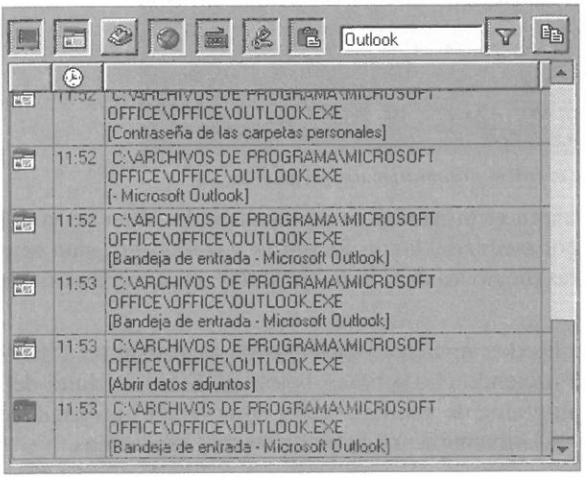
Para no se perderse entre protocolos de acciones muy extensos, Salus ha incorporado una práctica función de búsqueda, con la que puede delimitar las entradas visualizadas a aquellas que contengan un determinado concepto clave.

1. Al principio, lo mejor será que active todos los tipos de información.
2. A continuación, introduzca el concepto de búsqueda en el campo de entrada situado en la parte superior derecha. En nuestro ejemplo, vamos a emplear el concepto de búsqueda "Outlook", ya que queremos ver todas las entradas relacionadas con este programa de correo electrónico.



Introduzca en el campo de entrada un concepto clave para la búsqueda.

3. A continuación, haga clic sobre el botón *Filtro* situado a la derecha del campo de entrada. Salus filtrará todas las entradas en la lista de acciones y sólo dejará las que incluyan en alguna parte el concepto clave.



Así se pueden buscar determinados conceptos clave en las acciones protocoladas.

4. Para anular el efecto de filtrado y visualizar de nuevo todas las entradas, basta con hacer otro clic sobre el botón *Filter*.

Estas funciones le permiten saber siempre lo que ocurrió en su PC durante su ausencia. También puede emplear Salus para controlar a sus retoños internautas, o incluso para documentar sus propias acciones. Si, por ejemplo, ha perdido toda una página de texto por haberse producido una caída de Windows o del procesador de textos antes de que pudiera salvar el documento, tendrá bastantes probabilidades de poder reconstruirlo, al menos gran parte, con la ayuda de Salus, cosa que le ahorraría muchísimo de trabajo.

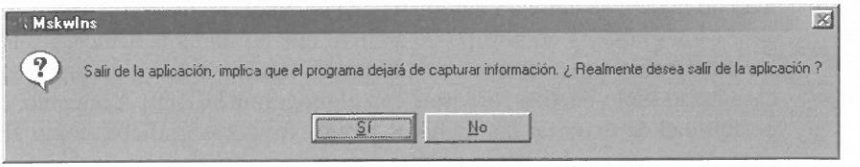
Desactivar Salus

Como el programa Salus va totalmente orientado a trabajar con discreción en segundo plano y no debe ser advertido por el usuario al que deseemos vigilar, no puede ser finalizado sin más. Hay que seguir un determinado procedimiento.

1. Llame primero al programa de administración de Salus, introduciendo la palabra secreta.
2. Ahora, con un clic sobre el botón *Propiedades*, situado a la izquierda del todo, abra la ventana de configuración y desactive allí la opción *Arrancar al iniciar Windows*. Así evitará que Salus vuelva a ser activado automáticamente la próxima vez que arranque Windows. Cierre las configuraciones con *Aceptar*.

Desactive el inicio automático del programa.

3. Finalice ahora el programa de administración. Pero no con la ocultación habitual por medio del botón *Esconder y continuar*, sino cerrando la ventana con las funciones de la barra de títulos o la combinación de teclas *[Alt] + [F4]*.
4. Confirme las dos siguientes consultas de seguridad para la conclusión del programa haciendo clic sobre el botón *Sí*. Esto concluirá definitivamente tanto el programa de administración como el de vigilancia de Salus, retirándolos de la memoria. Ya no se harán más vigilancias.



Confirme las consultas de seguridad para finalizar definitivamente el programa Salus.

Si quiere desactivar totalmente Salus, es importante que siga todos los pasos. Si por ejemplo, sólo finaliza el programa sin haber desactivado antes la configuración para que arranque automáticamente a la vez que Windows, el programa de control terminará temporalmente, pero la próxima vez que sea iniciado Windows se activará y volverá a recopilar datos.

Vigilancia automática de PCs no custodiados

Al comienzo de este apartado, ya establecimos una comparación con una cámara de vigilancia. Aunque en la práctica ésta resultaría poco eficaz, ya que, generalmente, no puede registrar la imagen visualizada en el monitor. Por una parte, esto se debe a que el usuario del PC casi siempre está sentado justo delante del monitor y, aunque no fuera así, con las cámaras habituales resulta casi imposible obtener desde una distancia de varios metros una imagen tan nítida que la grabación permita reconocer detalles de la pantalla. Por lo tanto, la clásica cámara de vigilancia queda descartada. Pero nada impide registrar lo que ocurre en la pantalla desde dentro, como quien dice. También aquí podemos instalar un programa que se ejecute clandestinamente en segundo plano y que a intervalos regulares (por ejemplo cada 60 segundos) haga y guarde una copia del contenido actual de la pantalla. Estas imágenes pueden ser evaluadas y analizadas después con toda tranquilidad. Delatan con absoluta exactitud lo que hizo el usuario, las aplicaciones y los documentos que abrió, las configuraciones que pudiera haber cambiado en el ordenador, o las páginas web que visitara desde el navegador.

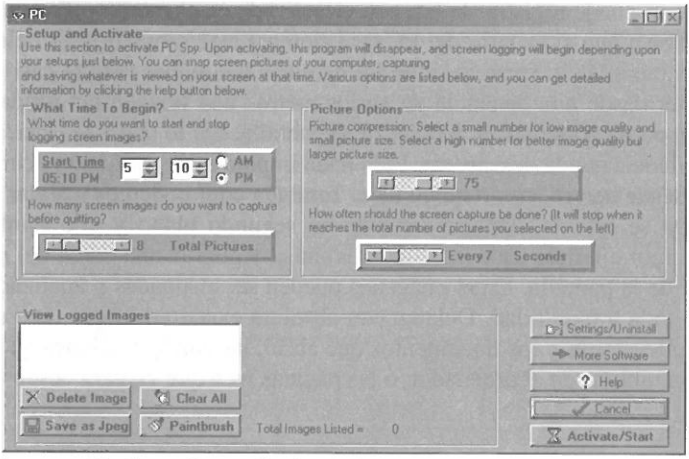
Vigilancia de video con PC Spy

Un programa de vigilancia visual de este tipo es *PC Spy*, que usted puede descargar en versión de prueba gratuita bajo la dirección http://www.softdd.com. El programa se ejecuta con absoluta discreción en segundo plano y no puede ser detectado ni parado, aunque se llame la lista de tareas de Windows con *[Ctrl] + [Alt] + [Supr]*. PC Spy puede ser configurado de tal manera, que a partir de un momento determinado empiece a generar y grabar cierta cantidad de copias de la pantalla. El tiempo entre dos copias puede ser ajustado a voluntad. El programa tampoco se deja interrumpir si entremedias, el PC es desconectado y conec-

tado de nuevo; se activará automáticamente en el momento oportuno. Las imágenes son grabadas en un tipo de archivo que no llama la atención y no puede ser reconocido como archivo de imágenes, aunque alguien se tope con él por casualidad. Sólo pueden ser vistas con el programa PC Spy. Asimismo, existe la posibilidad de exportar los archivos a otros formatos gráficos, como JPEG, en caso de ser requeridos como prueba.

Configurar PC Spy

Durante su instalación, el alojamiento estándar para PC Spy es el directorio *C:\Windows\Archivos de Programa\Softdd\PCS Spy*. No se generan entradas en el menú de inicio ni iconos en el escritorio de Windows. No en vano, la finalidad del programa es trabajar totalmente oculto y que, a ser posible, la persona vigilada no advierta nada. Para llamar al programa, arranque el archivo *pcs.exe* en el directorio mencionado más arriba. Las siguientes instrucciones le enseñarán a configurar PC Spy en pocos pasos, para que vigile sigilosamente toda actividad desempeñada en su PC.



La pantalla de configuración de PC Spy.

1. Si desea configurar PC Spy para su trabajo secreto, elija en primer lugar la hora de arranque a partir de la cual el programa deberá empezar a grabar el contenido de la pantalla. Para ello, seleccione en el área *What Time To Begin?* una hora, que vendrá indicada en el formato de horario americano. Es decir, sólo habrá que introducir la hora de 0 a 12 y añadir *AM* (antes de mediodía) o *PM* (después de mediodía) para aclarar si ésta se encuentra entre 0 –12 o entre 12 – 24 horas (del horario europeo). Ajuste la hora de arranque deseada, utilizando los campos de selección para horas y minutos y las opciones para diferenciar entre AM o PM.

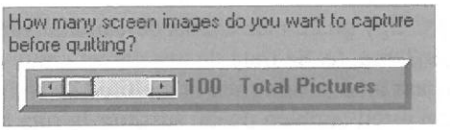
Ajuste en primer lugar la hora de arranque para el registro.

TRUCO

La hora de arranque correcta

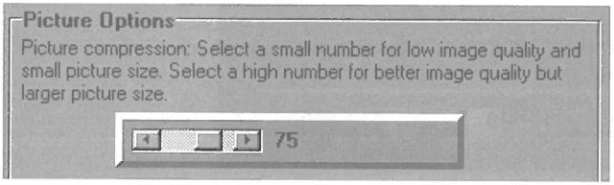
Cuando llega la hora de arranque, el PC comienza las grabaciones automáticamente. No importa si no está conectado en ese momento. Cuando sea puesto en marcha la próxima vez, PC Spy reconocerá automáticamente que la hora de arranque ha expirado e iniciará enseguida los registros. Lo que sí es importante es que el reloj interno de su PC esté bien ajustado, ya que el programa se orienta por él. Normalmente, la hora es visualizada en la parte inferior derecha de la pantalla, en la barra de inicio, de modo que usted la puede controlar desde allí. También se dispone de la opción *Fecha/hora* en la configuración del sistema, a la que se accede desde *Inicio/Configuración/Panel de control.*

2. Justo debajo, podrá indicar ahora cuántas copias de pantalla deberá hacer PC Spy en total. Con esta función se pretende evitar, sobre todo, que durante una larga sesión de trabajo con muchas tomas, se llene el disco duro de archivos de imagen. Usted puede solicitar un máximo de 9999 copias de pantalla. Aunque esto sólo basta para escasamente 14 horas de vigilancia en caso de elegir el intervalo de tiempo más corto (5 segundos) entre dos tomas.



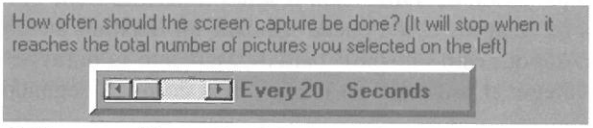
Especifique cuántas tomas deben hacerse en total.

3. Bajo *Picture Options*, puede ajustar primero la calidad de las imágenes registradas. Para ahorrar el máximo espacio en disco mientras trabaja, PC Spy aplica una compresión de los archivos de imágenes creados que, sin embargo, repercute en la calidad de la imagen. Cuanto menor sea el grado de calidad, más pequeños serán los archivos, pero más baja será también la calidad. Aunque con el valor estándar 75, ya se pueden obtener imágenes con una buena legibilidad. Nuestras pruebas han demostrado que se puede reducir la calidad hasta el factor 40 y seguir recibiendo imágenes claras.



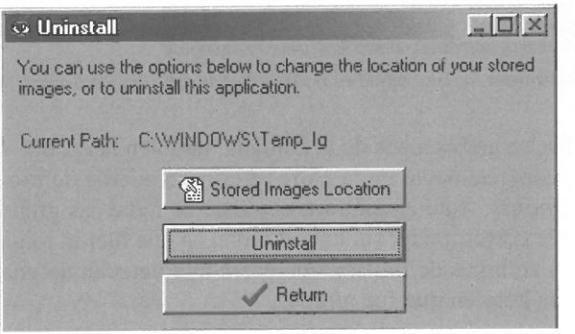
Con el factor de compresión, se ajustan el tamaño y la calidad de los archivos de imágenes guardados.

4. Debajo de la opción de calidad, encontrará finalmente la configuración más importante: la frecuencia con que debe generarse una toma. Para eso, seleccione en segundos el intervalo de tiempo que deba transcurrir entre dos tomas. El más pequeño es de 5, el más grande permitido de 900 segundos (15 minutos). La elección del intervalo depende del grado de exactitud con que usted quiera informarse de las actividades, o bien de las fechorías que espere del vigilado. La configuración de aprox. 120 segundos de intervalo entre las tomas, ya da una idea bastante fiel de lo que pueda hacer un usuario. Pero si lo que usted quiere es vigilar una sesión de navegación por la Red y quiere captar cada una de las páginas web visitadas, deberá elegir un intervalo más corto. Lo mismo vale si, prácticamente, quiere registrar una sesión de chat o la lectura y escritura de correos electrónicos.



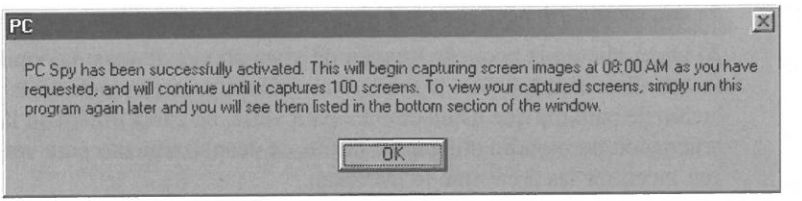
Indique a qué intervalos deberán realizarse las diferentes tomas.

5. De manera estándar, PC Spy guarda las copias de pantalla generadas en el directorio *C:\Windows\Temp_lg*. Se trata de una carpeta muy discreta, que en la mayoría de PCs pasa inadvertida entre la multitud de archivos y directorios temporales. Pero usted también puede sustituir la ruta de almacenamiento por otro directorio o unidad. Esto se hace abriendo con *Settings/Uninstall* la ventana *Uninstall*. Una vez allí, con un clic sobre el botón *Stored Images Location* se puede indicar otra ruta de almacenamiento.



En la ventana Uninstall, usted puede cambiar la ruta estándar para almacenar los archivos de imágenes.

6. Una vez hechas todas las configuraciones, puede activar PC Spy. Para eso, haga clic sobre el botón *Activate/Start*. El programa le presentará un último resumen de las configuraciones iniciales. Si usted las confirma haciendo clic sobre *OK*, PC Spy se retirará a su escondite en segundo plano.



Confirme el resumen de las configuraciones para activar definitivamente a PC Spy.

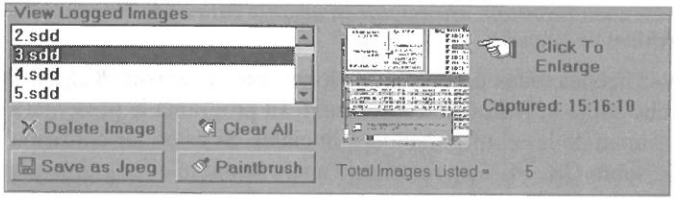
Ahora, el módulo de vigilancia de PC Spy estará activo en segundo plano, donde acechará hasta que llegue la hora previamente fijada. Entonces, activará la grabación y generará copias de pantalla según las configuraciones ajustadas. También esto transcurre en un segundo plano, de modo que el vigilado no advertirá absolutamente nada. El programa se ejecutará hasta que se alcance la cantidad de tomas especificada. Después, se desactivará automáticamente.

Análisis de las imágenes tomadas

Cuando PC Spy haya hecho sus grabaciones, usted podrá ver en todo momento las copias de pantalla generadas. Por lo tanto, deberá arrancar de nuevo el programa PC Spy con *pcs.exe*. Si en ese momento PC Spy aún estuviera activo (por no haber sido alcanzada la cantidad de tomas configurada), usted encontrará en el menú de configuración el mensaje *** Software Currently Activated*, así como el botón *Deactivate*. Podrá desconectar al espía siempre que quiera haciendo clic sobre el botón *Deactivate* y confirmando la consulta de seguridad que aparecerá a continuación.

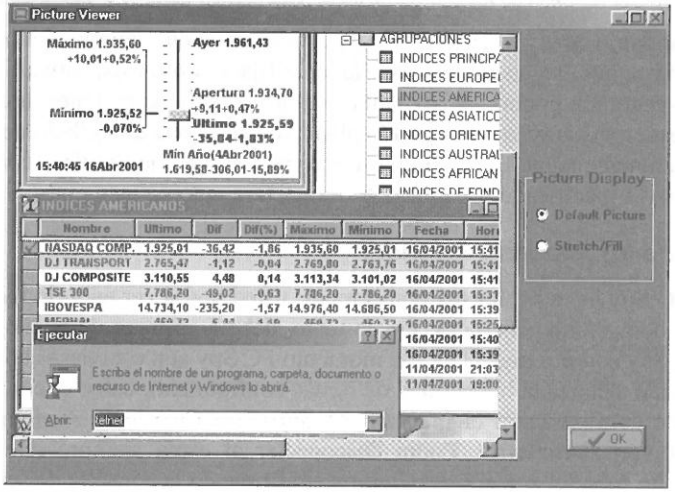
Si PC Spy aún estuviera activo, usted lo podría desconectar en cualquier momento con Deactivate.

Si PC Spy ha hecho grabaciones de la pantalla, también las podrá ver en la pantalla principal, concretamente en la parte inferior izquierda dentro del apartado *View Logged Images*. Aquí encontrará una lista de todas las grabaciones, cuya numeración suele corresponder sin más al orden en que fueron tomadas. Si usted elige uno de los archivos de la lista, aparecerá a la derecha de una vista previa de la imagen y la hora en que fue tomada.



En esta sección del menú principal puede ver las copias de pantalla tomadas.

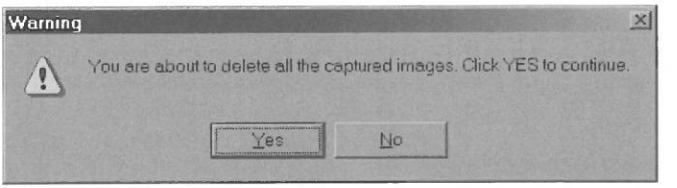
Al hacer clic en la pequeña imagen de vista previa, aparece la copia de pantalla en tamaño natural. Como la copia, normalmente, es generada en la misma resolución de pantalla que usted emplea para verla, no cabrá entera en la pantalla del ordenador, pero podrá utilizar las barras de desplazamiento para ver toda la imagen o centrar las áreas que le interesen.



Con la función Picture Viewer, puede ver a tamaño natural las imágenes tomadas.

Los cuatro botones situados debajo de la lista de imágenes facilitan las funciones más importantes para administrar y manipular las imágenes:

- *Paintbrush* arranca el programa que tenga definido en su PC como programa estándar para gráficos bitmap. Por regla general, es el programa de dibujo propio de Windows. Aunque puede ser que tenga configurado como estándar otro programa. Si al hacer clic sobre este botón no hay respuesta, significará que en su PC no hay instalado ningún programa de este tipo.
- Con *Save as Jpeg*, podrá guardar en formato JPEG la imagen que hubiera seleccionado en la lista. JPEG trabaja con un procedimiento de compresión muy bueno y genera archivos relativamente pequeños. A los archivos JPEG exportados de esta manera, no les afecta la función de borrado (véase más abajo).
- Haciendo clic sobre *Delete Image* se borra el archivo recién seleccionado en ese momento, quedando libre espacio en memoria.
- De modo similar, si bien con algo más de severidad, trabaja la función *Clear All*. Borra del disco duro todas las copias de pantalla que haya almacenadas en ese momento. Aunque antes hace una consulta de seguridad que habrá que confirmar haciendo clic sobre el botón *Yes*. Eso desencadena el borrado definitivo de los archivos de imagen (exceptuando los archivos JPEG que hubieran sido exportados previamente).



Confirme la consulta de seguridad para borrar las copias de pantalla almacenadas.

Para no malgastar espacio en memoria, le recomendamos emplear estas funciones con habilidad. Lo mejor será que compruebe regularmente las copias de pantalla generadas. Si hubiera entre ellas tomas "interesantes" que usted quiera emplear más adelante, guárdelas como archivos JPEG. A continuación, borre las copias restantes con *Clear All* para liberar espacio en memoria. Tenga en cuenta que si va menguando el espacio en el disco duro, al usuario vigilado se le podría ocurrir investigar la causa, con lo que se toparía con muchos archivos extraños que podrían despertar sus sospechas.

5. Contraataque – ¡Defiéndase!

5.1 ¡Abajo la máscara! – identificar al atacante 268
Ping – ¿Quién eres? 268
Traceroute – ¿De dónde vienes? 271
Whois – descubrir a los que están detrás 272
NeoTrace – análisis profesional 276

5.2 Si ya hemos agotado todos los recursos – ¿Devolvemos el golpe? 283
Ojo por ojo, diente por diente 283
Soluciones online para luchar contra los hackers 284
HackTracer – bloquear y denunciar a los hackers 286

5.3 Recursos legales contra los hackers 295
Persecución por vía penal 295
Persecución por vía civil 296

En este libro damos multitud de información sobre el modo de proceder de los hackers y cómo protegerse eficazmente de ellos, o cómo detectar los ataques a tiempo. Pero no queremos dejar fuera una cuestión que otras veces, por desgracia, se queda corta. ¿Qué podemos hacer si al final somos el objetivo de un ataque? Al fin y al cabo, no basta con detectar el ataque. Naturalmente, se puede emplear software de diversa índole, como por ejemplo un firewall personal, para chafar el éxito de la agresión. ¿Pero debemos dejar que el hacker quede impune y siga disparando tranquilamente sus torpedos digitales? Además, aparte de que el atacante pueda hacerse con un volumen considerable de datos de nuestro sistema, debido a los constantes ataques, cabe la posibilidad de que en algún momento éste pueda acabar encontrando un agujero de seguridad en el mismo. Y quizá usted no sea la única víctima. A lo mejor, los otros están mucho peor protegidos que usted. Por tanto, si pillamos a un hacker con las manos en la masa, deberíamos intentar darle un escarmiento.

En este capítulo vamos a ocuparnos de cómo identificar a quien nos está atacando desde Internet y de las diferentes posibilidades de poner fin a sus fechorías. Muchos de los métodos descritos también sirven en caso de ataques dentro de una red de empresa. Aunque aquí, hay de por sí muchas más oportunidades para defenderse. Una vez averiguada una dirección de la red como autora de los ataques, suele ser fácil dar con el "compañero" a quien fuera asignada esa dirección.

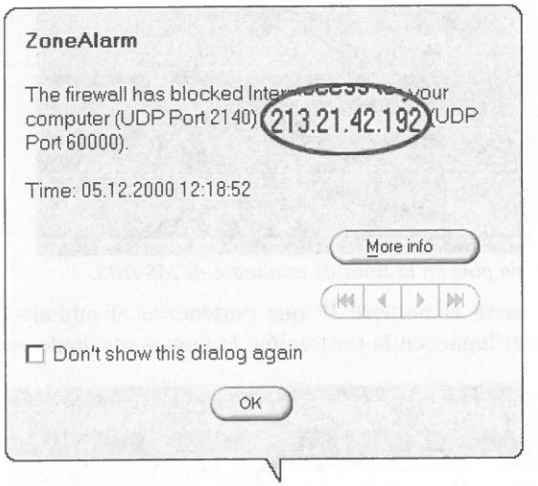
5.1 ¡Abajo la máscara! – identificar al atacante

El primer paso para la defensa es siempre la identificación del atacante. ¿Cómo vamos a defendernos o parar los pies a alguien, si no conocemos su identidad? En principio, averiguar el nombre real de la persona que está al otro lado de la línea es casi imposible, si no se cuenta con ayuda profesional. Pocos hackers van a ser tan torpes como para dejar alguna huella sobre su identidad. Salvo, naturalmente, que se trate de alguien al que usted ya conozca bastante y que se delate por determinadas acciones.

Pero como después de todo, el tráfico de datos en las redes no está basado en personas, sino que se produce entre máquinas, es posible averiguar la identidad del ordenador empleado. También se puede descubrir a qué dominio pertenece ese ordenador. Los responsables de los dominios son, en definitiva, personas, empresas u organizaciones concretas, que pueden ser investigadas hasta hallar a un contacto que nos ayude a buscar el autor verdadero. Un ejemplo sencillo: si un hacker se conecta telefónicamente a través del acceso call-by-call de un proveedor, al menos podremos averiguar quién es ese proveedor. Como aquí de momento nos estancaríamos, existiría la posibilidad de acudir a ese proveedor llevando los protocolos de los ataques del hacker. Si éstos suponen un delito, el propio proveedor podría investigar a partir de sus protocolos desde qué enlace tuvieron lugar esas conexiones telefónicas. De este modo, a partir de una dirección de ordenador se puede llegar hasta la identidad real de una persona.

Ping – ¿Quién eres?

El punto de partida para identificar a un atacante siempre es, al menos bajo Windows 9x/ME, disponer de un software especial. Ya sea una herramienta de protocolo que registre toda actividad en la red o un programa de protección, como podría ser un firewall personal, que reconozca los ataques y advierta sobre ellos. Otros sistemas operativos ya disponen de origen de un protocolo que refleja todas las incidencias importantes. La mayoría de los programas de protección incluyen, además, funciones de protocolo. Esto es muy importante, ya que sin protocolo resulta imposible demostrar posteriormente que hubo un ataque. Además, si se quieren revisar, por ejemplo, los protocolos de conexión telefónica de un proveedor, es imprescindible saber el momento exacto del ataque. Pero la información más importante es ante todo la dirección IP del ordenador atacante, que suele ser notificada o protocolada por el programa firewall.



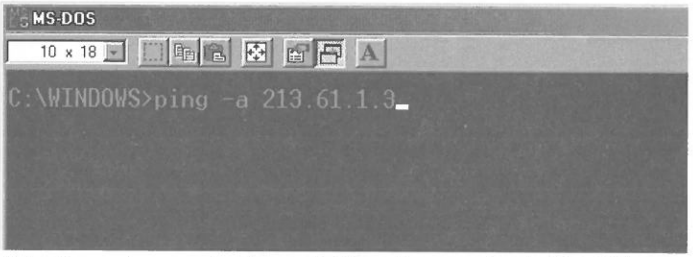
Cuando se produce un ataque, los programas de seguridad notifican el número IP del ordenador de donde partiera.

Este número IP supone el punto de partida para cualquier identificación, ya que proporciona la dirección de Internet del ordenador que fuera empleado por el atacante. Por desgracia, este número IP no es demasiado elocuente. Aunque la mayoría de los números IP tienen un compañero que es más revelador: el nombre IP. Con la ayuda del ***Domain Name Service*** (DNS), se puede descomponer un nombre IP en un número IP, o viceversa, averiguar a partir de un número IP el nombre IP correspondiente. La forma más sencilla de hacerlo es ***Packet Internet Groper***, que suele ser abreviado casi siempre como *ping* y viene incluido prácticamente en las funciones de cualquier sistema operativo moderno. Aunque Windows no conozca ninguna aplicación gráfica de *ping*, se puede introducir este comando en la línea de comandos de MS-DOS, con lo que ya es suficiente. Para averiguar mediante ping el nombre IP que corresponde a un número IP, proceda del siguiente modo:

1. Asegúrese de que su PC dispone de una conexión a Internet eficaz. Las consultas ping sólo se pueden hacer online.
2. Abra, después, el intérprete de comandos de MS-DOS e introduzca el comando ping, utilizando la siguiente sintaxis: *ping -a <Número IP>*. Si, por ejemplo, tuvo un ataque del número IP *213.613.1.3*, introduzca:

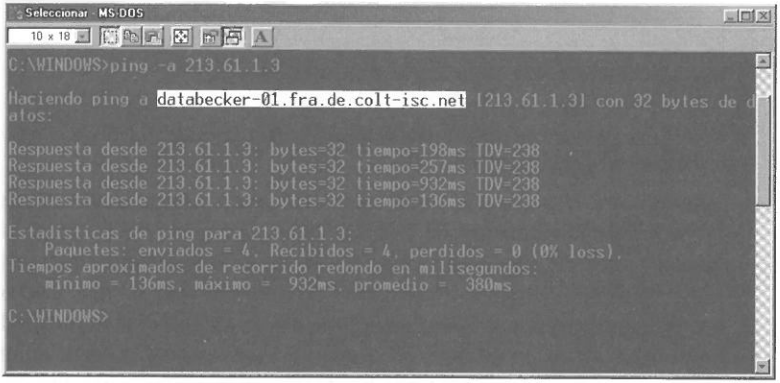
   ping -a 213.61.1.3

   Nunca olvide indicar la opción *–a*. Sólo así se investigará el nombre IP que corresponda al número IP.



Introduzca el comando ping en la línea de comandos de MS-DOS.

3. Ahora, ping averiguará el nombre IP que pertenezca al número IP y lo visualizará en primer lugar (en la ilustración, lo hemos resaltado en color).



Ping averigua a partir del número IP el correspondiente nombre IP.

4. Los datos siguientes tienen su origen debido a que ping investiga, después, la velocidad de conexión con ese ordenador de Internet. Esto no tiene gran relevancia para averiguar la identidad. Si la comprobación de la velocidad durase demasiado tiempo, cosa que puede ocurrir si el ordenador está muy lejos, podrá interrumpir el proceso con *[Ctrl] + [C]*.

5. Anótese el nombre IP averiguado para seguir utilizándolo y cierre la línea de comandos de MS-DOS, introduciendo *exit* y pulsando la tecla *[Intro]*.

Ahora, usted conoce el nombre del ordenador. Esto también incluye el dominio al que está asignado ese ordenador. Corresponde a las dos últimas partes que van separadas por un punto. Por lo tanto, en el nombre IP *www.server.provider.com*, el dominio sería *provider.com*. Con esta información, puede proseguir su búsqueda según vamos a explicarle dos apartados más adelante. Aunque, a veces, tampoco ping nos da el resultado deseado. Algunos números IP no se dejan convertir en nombres. En el siguiente apartado, le explicamos lo que puede hacer en este caso.

Traceroute – ¿De dónde vienes?

Si no ha habido éxito con ping, se puede probar con una herramienta parecida llamada *Traceroute*. También forma parte de las prestaciones de casi todos los sistemas operativos modernos. Su cometido es hacer un seguimiento de la conexión de Internet entre dos ordenadores, proporcionando información muy exacta sobre las estaciones intermedias a través de las cuales circulan los paquetes de datos. Esto nos puede dar una imagen del "vecindario" del ordenador atacante, aunque él mismo no revele información. En Windows, el correspondiente comando que se debe introducir en la línea de comandos de MS-DOS es *tracert*. Se emplea del siguiente modo:

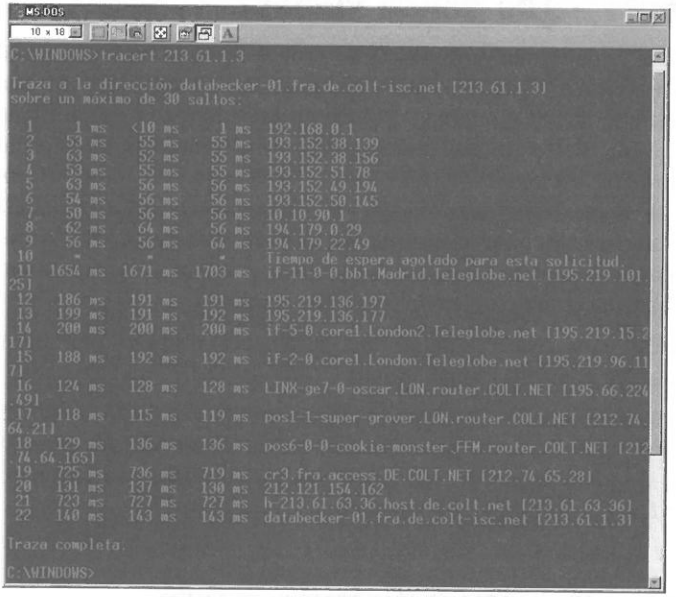
1. También para *tracert* tendrá que establecer primero una conexión a Internet, ya que sólo trabaja online.

2. Abra a continuación la línea de comandos de MS-DOS e introduzca el comando tracert con la siguiente sintaxis: *tracert <IP-Number>*. Por lo tanto, si quiere seguir el recorrido hasta el ordenador cuyo número IP sea *213.61.1.3*, introduzca el comando:

   tracert 213.61.1.3

Introduzca el comando traceroute en la línea de comandos de MS-DOS.

3. Ahora, traceroute iniciará un seguimiento del recorrido de los datos desde su propio PC hasta el ordenador cuyo número IP coincida con el indicado. Empezará con la estación más próxima a su ordenador y saltará después de un ordenador a otro. Para cada estación intermedia, el programa volverá a emitir el número IP del ordenador implicado y – siempre que lo pueda averiguar – el nombre IP.



Estos son los resultados del análisis de conexiones realizado por traceroute.

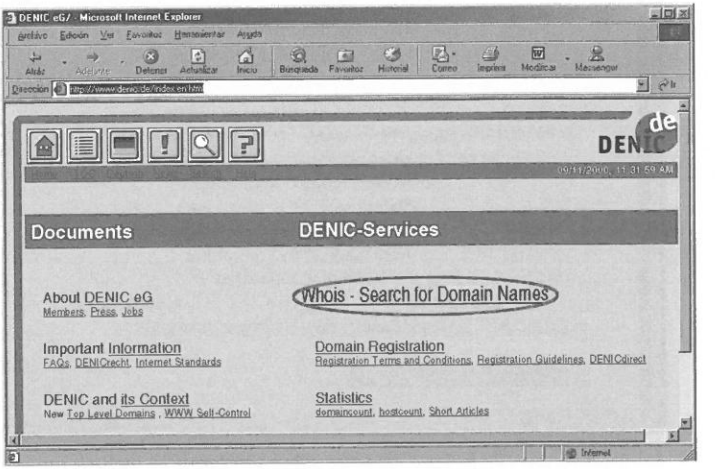
Si para el número IP buscado con ping no se pudo hallar ningún nombre IP, tampoco lo logrará traceroute. Pero hay una probabilidad bastante elevada de que traceroute pueda averiguar los nombres IP de los vecinos más próximos del ordenador atacante. Éstos ya suelen pertenecer a la red del mismo proveedor, de modo que también en este caso se es posible obtener un nombre de dominio. Un número IP cuyo comienzo sea igual o parecido, también es un indicio de que ambos ordenadores pertenecen a la misma red. No obstante, si se ha averiguado de esta manera un nombre de dominio, habría que aclarar con el proveedor si el ordenador en cuestión pertenece realmente a su red. Pero, en cualquier caso, existe una relación inmediata, de modo que el propietario del dominio debe conocer al operador del ordenador.

Whois – descubrir a los que están detrás

Un dominio no siempre sirve de ayuda. En cualquier caso, usted puede intentar averiguar si el dominio averiguado tiene una página web. Si usted posee, por ejemplo, el dominio *provider.com*, ¿por qué no introduce la dirección http://www.provider.com en su navegador web? Con un poco de suerte existirá una página web para ese dominio y éstas suelen indicar en su pie de página posibilidades para contactar con su operador. Si este camino no ha tenido éxito, aún disponemos de otra forma de averiguar el operador de un dominio. Las entida-

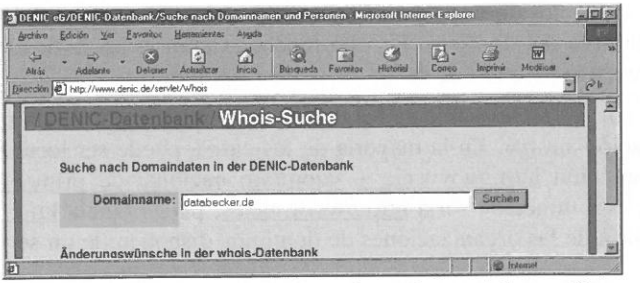
des responsables de organizar los dominios de primer nivel, (*.com*, *.es*, *.net*, etc.) llevan bases de datos sobre los dominios que están registrados bajo el respectivo dominio de primer nivel. Ningún operador de dominio puede escapar a este registro. Estas bases de datos pueden ser consultadas en línea a través de Internet. Si, por ejemplo, el dominio buscado es alemán y el sufijo es *.de*, podrá dirigirse a *DENIC*, responsable de organizar los dominios alemanes de primer nivel.

1. Cargue desde su navegador la página web *DENIC*, bajo la dirección http://www.denic.de/index.en.html. Seleccione, en la página inicial, el punto de menú *Whois-Search for Domain Names* (Búsqueda Whois por nombre de dominio).



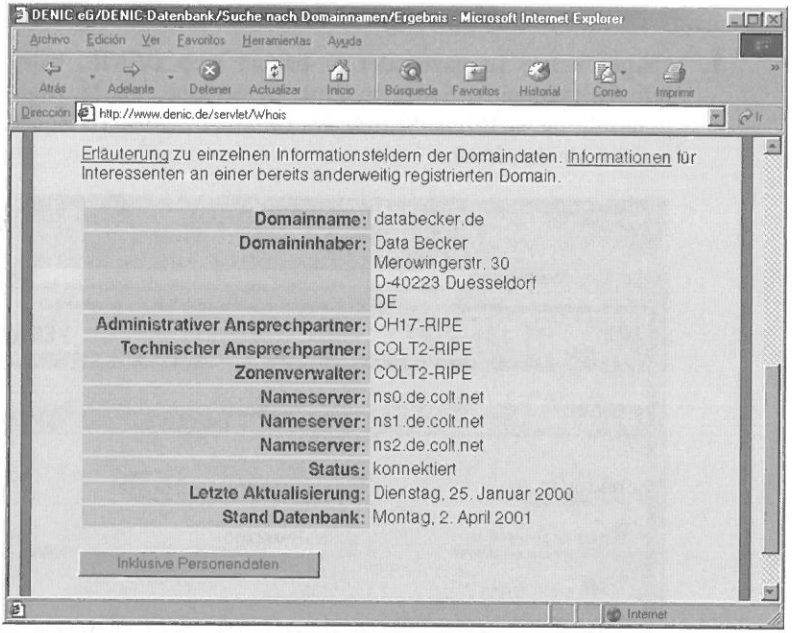
En la página inicial de DENIC encontrará la opción Whois – Search for Domain Names (Búsqueda Whois por nombre de dominio).

2. Con esto, entra en el menú de búsqueda, donde deberá introducir el dominio sobre cuyo operador desee informarse, haciendo después clic sobre el botón *Suchen* (Buscar).



Introduzca el dominio sobre el que desee obtener información.

3. A continuación, tendrá lugar la exploración del dominio indicado en la base de datos de DENIC y la creación de una página de resultados con la información esencial sobre el propietario del mismo. Por regla general, bajo propietario del dominio encontrará el nombre y la dirección de la empresa que registró y explota ese dominio.



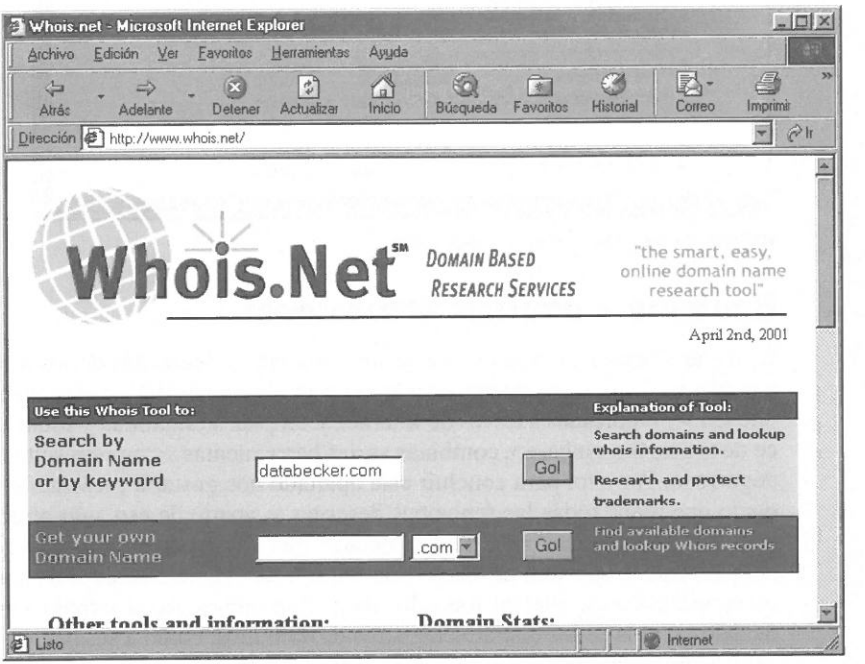
La información de la base de datos sobre un dominio incluye nombre y dirección del propietario.

4. Si todo esto aún resulta insuficiente, haciendo clic sobre el botón *Inklusive Personendaten* (Incluir datos personales) situado en la parte inferior, podrá solicitar una versión más completa del resultado de búsqueda. Ésta proporciona también el nombre y quizá las direcciones y números de teléfono de los contactos directos que estén a cargo del mantenimiento técnico o administrativo del dominio. De este modo, existirá la posibilidad de contactar directamente con una de las personas responsables.

DENIC sólo es responsable de los dominios alemanes, pero cada país tiene una organización similar. En la mayoría de los casos, puede ser localizada a través de la dirección http://www.nic + <dominio nacional de primer nivel>. Para España, esta dirección sería http://www.nic.es, para Francia http://www.nic.fr. La mayoría de las organizaciones de dominios disponen de un servicio de bús-

queda en línea. Si no fuera así, usted podría intentar solicitar la información deseada por correo electrónico.

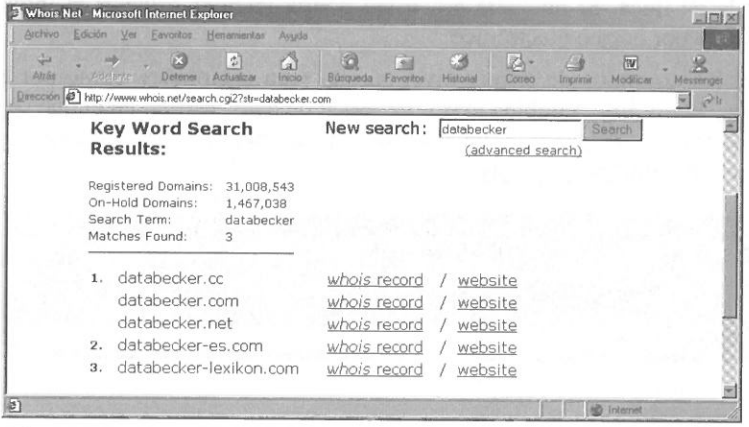
Para los dominios de primer nivel que no sean nacionales, como por ejemplo *.com*, *.net* o *.org* , también existe un banco de datos central en el que se pueden consultar los propietarios de dominios. Éstos pueden ser contactados bajo la dirección http://www.whois.net



www.whois.net ofrece un servicio para buscar la información de dominio para diferentes dominios de primer nivel.

Aquí se encuentra ya en la página inicial un formulario de búsqueda, donde simplemente tendrá que introducir el dominio a buscar y hacer clic sobre *Go!*. Si hay varios dominios que coincidan con la búsqueda, entonces recibirá primero una relación de todos los candidatos.

En la página de resultados elija el dominio concreto sobre el que desee informarse. A continuación, recibirá todos los datos disponibles sobre el operador de ese dominio.



Elija en la relación el dominio buscado.

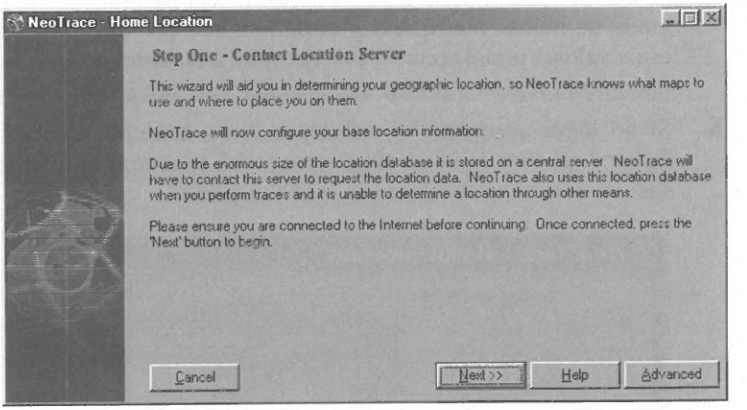
NeoTrace – análisis profesional

Hasta aquí hemos presentado varias herramientas procedentes de los medios de a bordo, es decir, que pertenecen a la gama de funciones del sistema operativo o pueden ser empleadas a través de Internet. Cumplen su finalidad y están al alcance de todos. Sin embargo, combinar varias herramientas siempre resulta un poco engorroso. Por ello, para concluir este apartado nos gustaría presentarle un producto que reúne todas las funciones descritas y, aparte de eso, aún ofrece algunas ventajas prácticas más. Podría decirse que *NeoTrace* es el modelo de lujo para analizar un circuito de datos. Una vez introducida la dirección IP, nos muestra en una eficiente interfaz todos los datos disponibles. Accede tanto a las bases de datos Whois de los distintos registros de dominios, como a sus propios mapas para representar gráficamente el recorrido hasta el ordenador buscado y el emplazamiento del mismo. En la dirección http://www.neotrace.com, podrá descargar sin coste alguno una versión de prueba.

Instalar y preparar NeoTrace

NeoTrace viene como un programa de instalación automática, cuyas fases se desarrollan de manera habitual. Por regla general, después de la instalación no hace falta reiniciar el ordenador. Más adelante, cuando se haga el primer arranque, habrá que indicar al programa el propio emplazamiento. Esta información la necesita para poder representar correctamente en un mapa la conexión con el ordenador objetivo. Para hacer esta configuración, el propio programa inicia automáticamente un asistente, que le guiará a usted por todos los pasos.

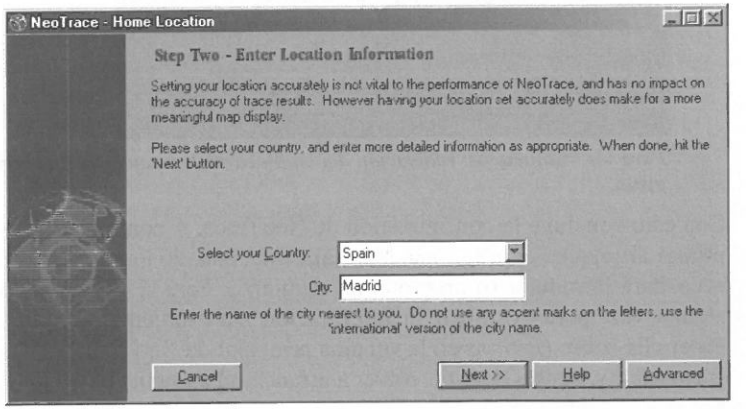
1. Al arrancar, será saludado por el asistente con un breve mensaje. Importante: para que el asistente pueda acceder luego a la base de datos de emplazamientos, deberá haber una conexión activa. Por lo tanto, conéctese a Internet y haga clic sobre el botón *Next* para avanzar al siguiente paso.



Conéctese a Internet, antes de que el asistente de emplazamientos empiece a trabajar.

2. Seleccione primero, en el campo *Select your Country*, su país de procedencia. Tenga en cuenta que aquí, los países vienen con su denominación inglesa, por ejemplo Spain, Germany o Switzerland.

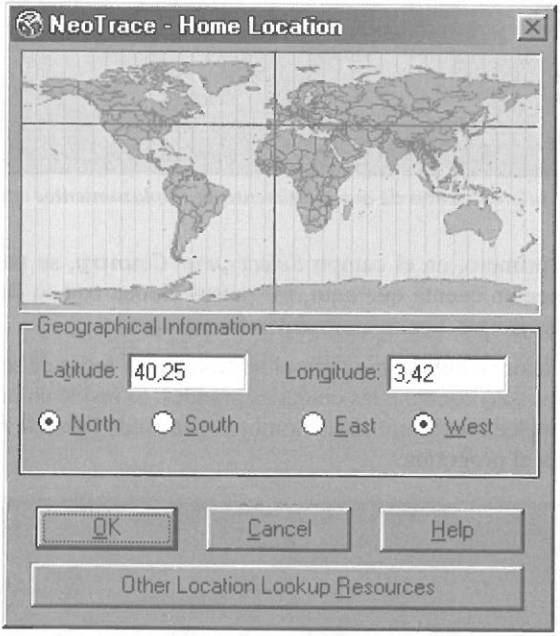
3. Introduzca ahora en el campo *City* el nombre de su lugar de residencia. La base de datos sólo contiene las ciudades grandes. Si reside en una población pequeña, emplee sencillamente el nombre de la ciudad grande más próxima que conozca el programa.



Indique su país de procedencia y la ciudad grande más próxima.

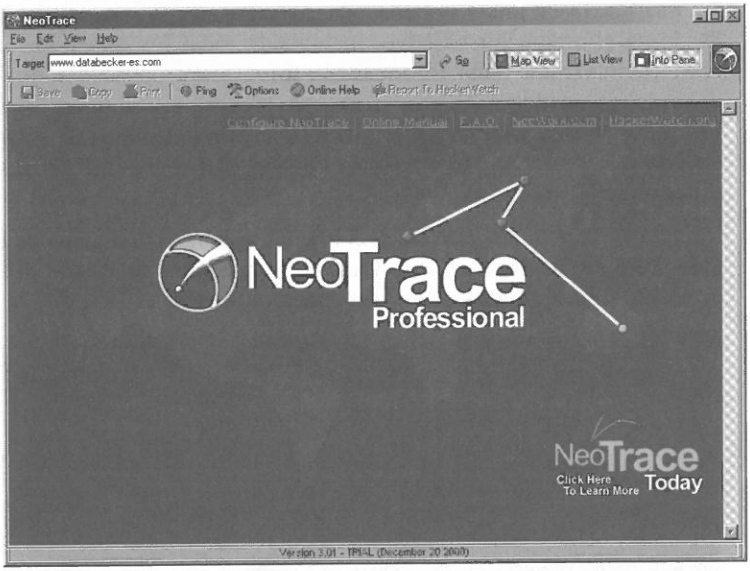
4. Si la ciudad más próxima conocida está demasiado lejos o, por alguna otra razón, no está satisfecho con el resultado, también puede indicar su ubicación con toda exactitud. Para ello, haga clic sobre el botón *Advanced*. Con esto cerrará el asistente y, en su lugar, abrirá una amplia ventana donde podrá introducir con absoluta precisión su emplazamiento, incluyendo el grado de latitud *(Latitude)* y el de longitud *(Longitude)*. Para averiguar estos valores podrá recurrir, por ejemplo, a un sistema GPS, un mapa detallado de su región o probar en la página web http://www.mapblast.com.

5. Si no logra averiguar los valores exactos, haciendo clic sobre el botón *Other Location Lookup Resources* podrá encontrar en Internet los recursos y la información necesaria a este respecto.



Para los minuciosos: indicación del emplazamiento con grado de latitud y de longitud.

Con esto concluye la configuración de NeoTrace. A continuación, tiene lugar el primer arranque del programa. Naturalmente, cuando lo inicie en el futuro ya no necesitará introducir su propio emplazamiento. Pero si su ordenador se mudara alguna vez, podrá cambiar la información sin problema; simplemente deberá hacer clic sobre *Options* en la ventana principal de NeoTrace, cambiar a la categoría *Map* y, dentro de ésta, volver a arrancar al asistente de emplazamiento con *Set Home Location*.

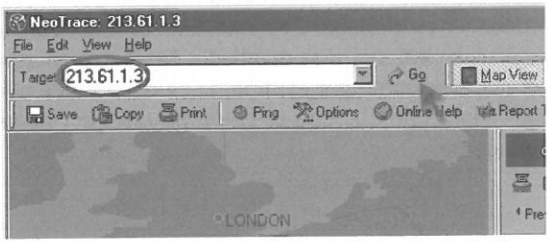


Una vez configurado el emplazamiento, NeoTrace arranca automáticamente por primera vez.

Hacer un seguimiento de las conexiones con NeoTrace

Para hacer mediante NeoTrace el seguimiento de una conexión con el ordenador sospechoso y averiguar su identidad, sólo necesitará un número IP, igual que ocurre con ping o trace.

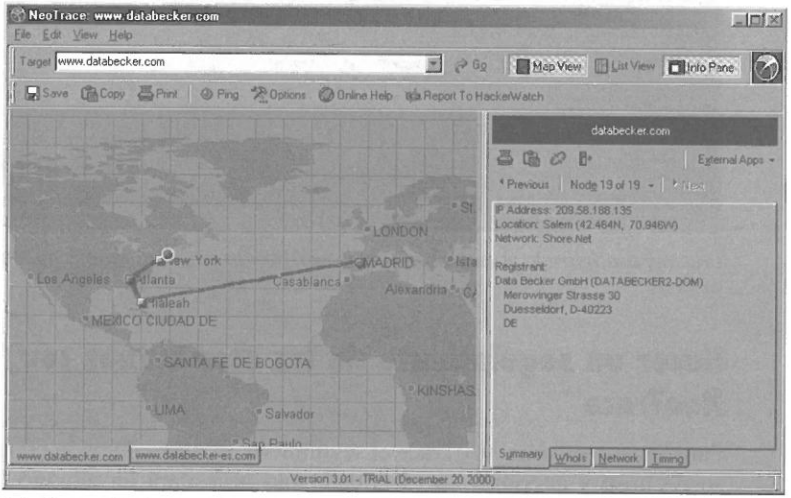
1. Introduzca el número IP sospechoso o una dirección IP en la parte superior de la ventana de NeoTrace, concretamente en el campo *Target*. Después, haga clic sobre el botón *Go*.



Para arrancar la búsqueda, introduzca en el campo Target el número o nombre del ordenador sospechoso.

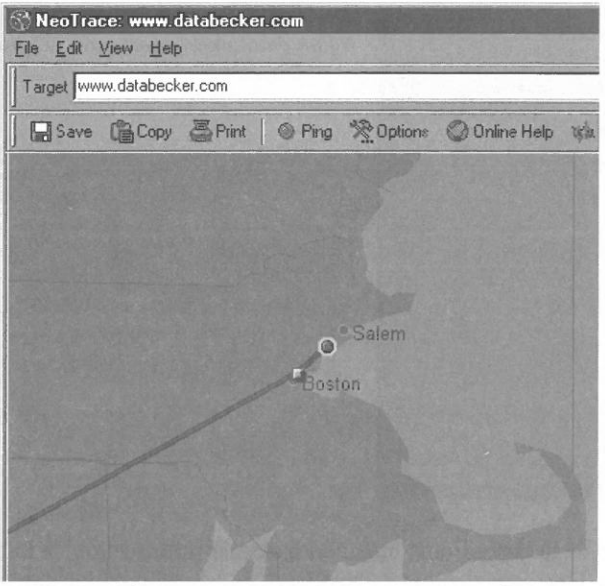
2. Ahora, NeoTrace inicia la búsqueda, averiguando la ruta exacta desde su PC hasta el ordenador objetivo, incluyendo todas las estaciones intermedias. Suministrará tanta información sobre los ordenadores implicados, como le sea posible conseguir. Todo este proceso puede llevar algún tiempo, en función de las estaciones intermedias. En la ventana de información situada a la derecha, podrá seguir el avance del proceso y la cantidad de ordenadores explorados.

3. Ya durante el análisis, NeoTrace comienza a elaborar un mapa de la conexión. Para eso dispone en *Map View* de un mapamundi, donde va dibujando los diferentes ordenadores y las conexiones entre ellos.



NeoTrace dibuja en un mapamundi la conexión con el ordenador objetivo.

4. Como se supone que a usted le interesará, sobre todo, el último ordenador situado al otro extremo de la conexión, puede emplear la función zoom del mapa para visualizarlo a gran escala. Para ello, basta con que haga hasta siete veces clic con el botón izquierdo del mouse sobre la posición que ocupe este ordenador en el mapa. Con cada clic, el fragmento se irá haciendo más pequeño y se volverá más detallado, hasta que finalmente se puedan reconocer detalles, como por ejemplo la ciudad grande más próxima al emplazamiento. Haciendo clic con el botón derecho del mouse, volverá a aumentar el encuadre.

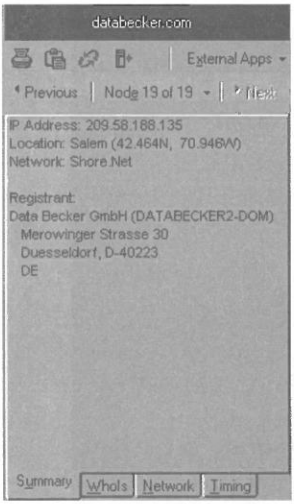


Con la función zoom, usted puede visualizar con más detalle el emplazamiento de cada ordenador.

5. Si hace clic directamente sobre la ubicación de un ordenador (por ejemplo, sobre el ordenador objetivo) sin que el puntero del mouse se transforme en una lupa, podrá solicitar más información sobre ese ordenador. Si en ese emplazamiento hubiera varios ordenadores que participen en la conexión, aparecerá en el mapa un pequeño menú con la selección de esos ordenadores.

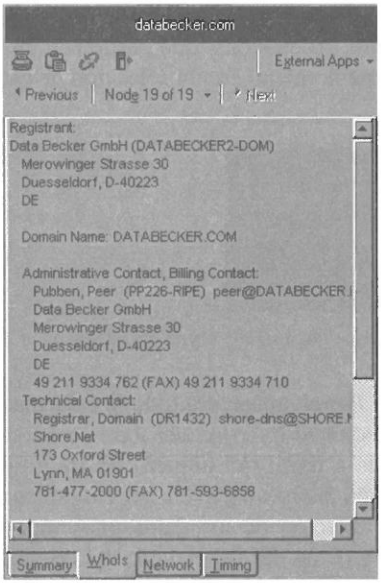
Si hay varios ordenadores implicados, introduzca el que desee en el menú de selección.

6. En la parte derecha de *Info Panel*, aparecerá toda la información disponible sobre el ordenador seleccionado. Arriba del todo aparecerá el nombre IP, si ha podido ser derivado a partir del número IP. La información que viene desglosada en la pestaña *Summary* suele ser casi siempre la categoría más útil. Contiene una relación de los datos más importantes; si se encuentra disponible una dirección del propietario del dominio, aparecerá aquí.



En la categoría Summary de Info Panel encontrará los datos más importantes del ordenador.

7. Dentro de la categoría *WhoIs* podrá extraer información de la base de datos Whois. Una gran ventaja de NeoTrace es que solicita los datos automáticamente en función del dominio de primer nivel, de modo que usted no tendrá que discurrir qué organización podría ser responsable de cada dominio de primer nivel.



NeoTrace también facilita los datos de la base de datos Whois.

5.2 Si ya hemos agotado todos los recursos – ¿Devolvemos el golpe?

En la primera parte de este capítulo nos hemos ocupado de cómo averiguar la identidad del atacante, o la del ordenador empleado. Ahora queremos contestar a la pregunta de qué hacer con esa información.

Ojo por ojo, diente por diente

Desde luego, lo primero que se nos podría ocurrir sería pagar al atacante con la misma moneda. A fin de cuentas, conociendo la dirección IP del ordenador empleado por éste, es absolutamente factible aplicar el programa apropiado para contraatacar. Pero nos gustaría desaconsejarle algo así, por muchas ganas que le pueda tener al atacante. Hay varias razones que hablan en contra de semejante acción de venganza. A continuación, vamos a exponerlas brevemente.

Mantenga su conciencia limpia

La cita "Ojo por ojo, diente por diente" es una perífrasis de venganza empleada en el Antiguo Testamento de la Biblia. Ya en aquellos tiempos, no daba muy buen resultado. Por eso, miles de años después se editó el Nuevo Testamento, donde el lema era "¡Pon la otra mejilla!". Esto no quiere decir que deba permitir a los hackers seguir impunemente con sus fechorías, pero pagar con la misma moneda no conduce a nada. Por una parte, ya podrá imaginar que un hacker medianamente inteligente se protegerá de los contraataques. De modo que usted se esforzaría para nada. Por la otra, con tales contramedidas quizá aún incitaría más al atacante, desatando así una guerra de información en toda regla. Y, por cierto: si usted emplea las mismas armas que el atacante, no será mucho mejor que él, ¿no?

Mantenga su integridad

Desde el punto de vista legal, los hackers se mueven en terreno resbaladizo. El último apartado de este capítulo abordará con más detalle qué se puede hacer y qué está prohibido. Si usted emplea los mismos métodos y herramientas que ellos, pisará también ese terreno resbaladizo. La manipulación y destrucción de datos ajenos es un acto delictivo y puede ser perseguida por vía penal y civil. Como habrá visto en este capítulo, también en el anónimo Internet es absolutamente posible descubrir al autor de un ataque; no piense que no le van a pillar. Además, con una acción así, usted mismo se privaría de la oportunidad de proceder legalmente contra un hacker.

Respete a los inocentes

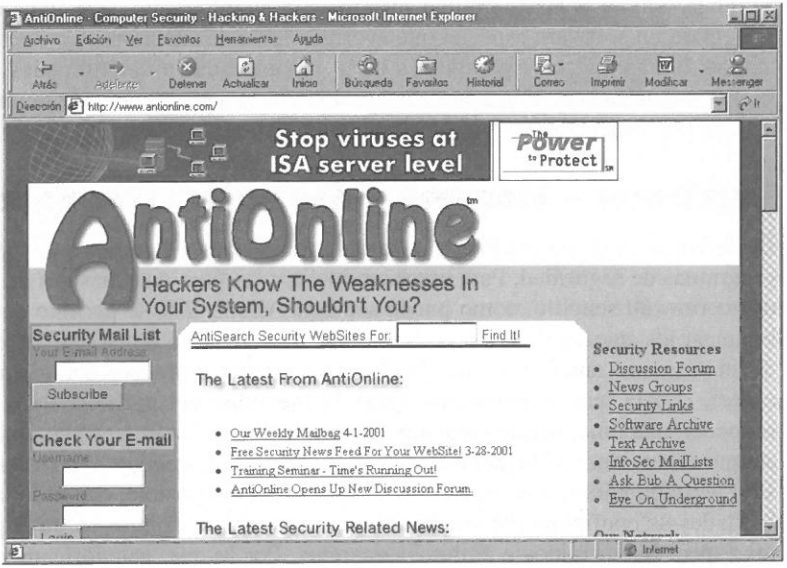
Finalmente, un argumento convincente para disuadirle de lanzar su contraataque, es que nunca podrá estar seguro de haber hecho blanco contra la persona correcta. Al fin y al cabo, los ataques hacker no van dirigidos directamente a personas concretas, sino a ordenadores y redes, y el hacker no tiene por qué ser el único usuario de un ordenador o una red. De modo que, si usted inicia por ejemplo un ataque *Denial of Service*, lo más seguro es que también afecte a terceros inocentes. Asimismo, podría ser que el hacker ni siquiera lanzara el ataque desde su propio ordenador, sino que recurriera, por ejemplo, a un troyano instalado en el ordenador de alguien que ignora lo ocurrido. En este caso, su investigación habría sacado a la luz la dirección de un implicado que no tiene culpa de nada. Si usted le ataca, al hacker no le haría daño, pero perjudicaría al desprevenido propietario del ordenador que fuera usado ilícitamente.

Como habrá podido ver, existen buenas razones para no rebajarse a la categoría moral del atacante, y aunque no contraataque, usted no está del todo desamparado. Por un lado, podrá dirigirse al operador de redes desde cuyo ordenador actúe el hacker. Por el otro, en Internet hay páginas que le apoyarán en su lucha contra los hackers. Éstas se basan en la idea "Juntos tenemos fuerza" y analizan las denuncias de muchos usuarios para reconocer pautas en los ataques de los hackers y probar así la culpabilidad de malhechores notorios.

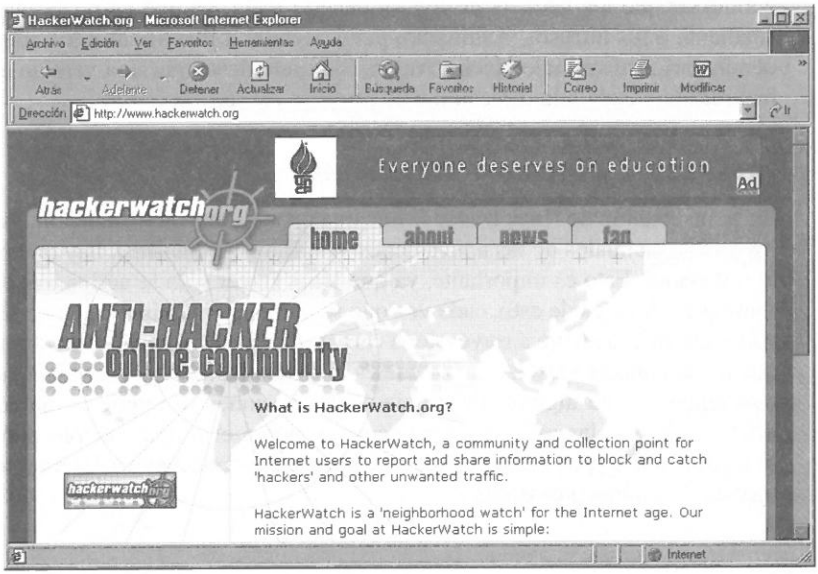
Soluciones online para luchar contra los hackers

Una página muy informativa es *AntiOnline*, que podrá encontrar en la dirección http://www.antionline.com . Ofrece multitud de información útil para la lucha contra los hackers. Aquí podrá encontrar también informes actuales sobre ataques y consejos detallados para descubrir a los hackers. Además, desde aquí tendrá acceso a foros de discusión sobre el tema, donde podrá intercambiar información con otros afectados. Completan la oferta recopilaciones de links y listas de mailing sobre el tema.

Aún más completa es la página *HackerWatch* bajo la dirección siguiente http://www.hackerwatch.org. Esta página cuenta con una base de datos central con amplia información sobre ataques de hackers. Esta base de datos es analizada continuamente para buscar pautas en la información de los ataques. Si se reconocen pautas, por ejemplo cuando varios usuarios estén siendo atacados desde la misma dirección, HackerWatch informará a los afectados y hará posible que establezcan contacto entre ellos. De este modo, se puede proceder colectivamente contra los atacantes, y a la hora de iniciar acciones legales, las perspectivas de éxito son infinitamente mejores. Las autoridades toman mucho más en serio a hackers que actúen regularmente contra muchas víctimas, que a los autores de una sola vez u ocasionales.



AntiOnline ofrece mucha información para la lucha contra los hackers.



HackerWatch recopila y analiza de manera centralizada la información de ataques procedentes de todo el mundo.

Si quiere enviar a HackerWatch información sobre ataques que haya sufrido, necesitará un software especial que averigüe los datos necesarios y los transmita. Las funciones correspondientes están incorporadas a determinados programas de seguridad. En el siguiente apartado, vamos a presentarle un programa de esta índole, especialmente desarrollado para rastrear hackers.

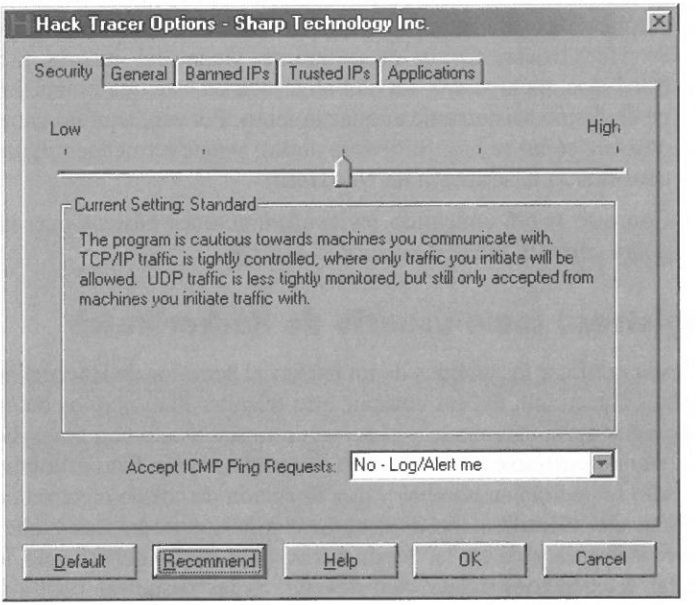
HackTracer – bloquear y denunciar a los hackers

HackTracer es un producto que aúna las propiedades y funciones de diferentes programas de seguridad. Para empezar, incluye las funciones básicas de un producto firewall sencillo, como puede ser ZoneAlarm. Esto le permite detectar y bloquear los ataques de hackers. A esto hay que añadir la funcionalidad esencial de un programa analítico como NeoTrace (HackTracer procede del mismo fabricante), con la que se puede averiguar la identidad del agresor. Todo esto lo redondea una función que mediante un simple clic de ratón, permite notificar el ataque al servidor de HackerWatch (vea el apartado precedente). El programa ha sido pensado para que su manejo sea lo más sencillo posible, evitando las posibilidades de configuración ampliadas que se pueden encontrar en otros productos especiales dirigidos a ámbitos concretos. Por lo que, categóricamente, NO recomendamos su empleo como único programa de seguridad. Aunque sí resulta muy indicado si tiene problemas concretos con hackers. En tal caso, puede garantizar que los hackers no logren hacerle daño, ya que cierra la puerta eficazmente a los intrusos. Asimismo, puede ayudar a identificar a los atacantes y denunciarlos al servicio HackerWatch. Si quiere descargar una versión de prueba gratuita, acuda a la dirección web http://www.neoworx.com.

Instalar y preparar HackTracer

De la instalación de HackTracer se encarga un asistente de instalación, que sigue los pasos habituales de las aplicaciones Windows. Al finalizar, hay que reiniciar el ordenador. Esto es importante, ya que HackTracer sólo se activa tras el nuevo arranque. Después de esto, cada vez que se ponga en marcha Windows será activado automáticamente a través de la carpeta *Inicio*. En el primer arranque habrá que hacer algunos ajustes, sin los cuales el programa no podrá ser manejado adecuadamente. Para algunas de las siguientes acciones se requiere una conexión activa. Además, las ayudas y explicaciones sobre el programa sólo pueden ser llamadas online, por lo que resulta recomendable conectarse a Internet antes de ejecutar los siguientes pasos.

1. La primera vez que se inicia HackTracer, se abre automáticamente el menú de configuración con la categoría *Security* visible.



Seleccione el estado de seguridad que HackTracer deba implantar en su ordenador.

2. Utilizando la barra deslizante situada en la parte superior, dispondrá de varios niveles para elegir el grado de seguridad que quiera implantar en su ordenador.

TRUCO

El nivel de seguridad adecuado para HackTracer

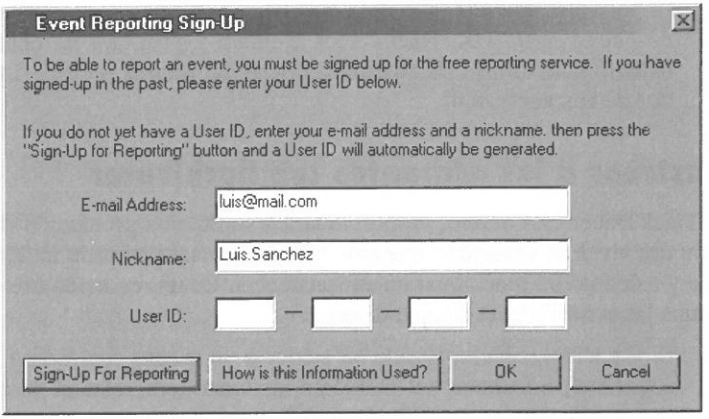
Si desliza el regulador hacia el extremo de la izquierda (*Current Setting: Open*), prácticamente desactivará del todo la función de protección de HackTracer. Por supuesto, esto no es nada recomendable, aunque podría resultar conveniente temporalmente si un programa de Internet está siendo obstaculizado. El extremo contrario estaría a la derecha del todo (*Current Setting: Lock-Down*). Con él, se interrumpe rigurosamente cualquier tráfico de su ordenador dentro de Internet. Aunque en este modo no se avisa de ningún ataque de hackers. Como siempre, lo mejor es el término medio. Con *Current Setting: Standard*, proporciona a su PC una protección fiable, ya que sólo permitirá el tráfico de datos con el exterior, si es usted quien lo ha iniciado. Si tiene lugar un intento de establecer contacto no provocado por usted, HackTracer lo considerará un ataque y pondrá en marcha su mecanismo de protección. Si ve que con las configuraciones actuales HackTracer desencadena demasiadas falsas alarmas, podrá evitarlas, casi siempre, reduciendo el nivel de seguridad.

3. Cuando haya seleccionado un nivel de seguridad, debería cambiar a la categoría *General*, en cuya parte inferior encontrará el botón *Change Home Location*. Este botón le permite arrancar un asistente para definir el propio emplazamiento, necesario si quiere emplear la función gráfica Traceroute de HackTracer. Como el programa viene del mismo fabricante que NeoTrace, incluye una versión aligerada de éste que prácticamente contiene el mismo asistente de emplazamiento. Por eso, aquí no vamos a explicar otra vez cómo se usa. Si tuviera dudas, puede retroceder algunas páginas y consultar la descripción de NeoTrace.
4. Con esto habrá concluido las configuraciones básicas más importantes y podrá cerrar el menú de opciones con *OK*.

Regístrese como usuario de HackerWatch

Si desea notificar los ataques de un hacker al servidor de HackerWatch, a través de HackTracer, aún deberá cumplir otro trámite. Para que los datos puedan ser procesados apropiadamente y el servicio no sea usado con fines ilícitos, primero hay que registrarse en HackerWatch como usuario. Esto es totalmente gratuito y sólo le pedirán su nombre y una dirección de correo electrónico. A cambio, le darán una identificación de usuario con la que podrá hacer que HackTracer genere informes y los envíe. Según afirma el operador del servicio, los datos personales reciben tratamiento confidencial. Si las pesquisas contra un hacker lo requirieran, serían remitidos a los órganos instructores u otras personas autorizadas. Aunque antes, siempre le informarían y le pedirían la correspondiente autorización.

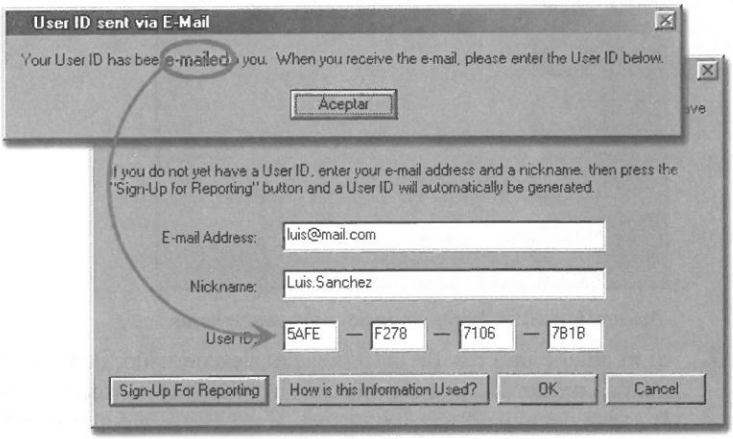
1. Para registrarse como usuario en HackerWatch, ejecute – desde la ventana principal de HackTracer – la secuencia de menú *Event/Report User Settings...*
2. De esta forma abrirá la ventana *Event Report Sign-Up*, donde deberá indicar en el campo *E-mail Address* una dirección de correo electrónico válida.
3. Debajo de ésta, introduzca en el campo *Nickname* su nombre o alias.



Para registrarse, introduzca su dirección de correo electrónico y su nombre.

4. Si su PC aún no tuviera una conexión activa con Internet, deberá establecerla ahora. Es imprescindible para el siguiente paso.

5. Ahora, haga clic sobre el botón *Sign-Up For Reporting*. El programa comunicará los datos personales introducidos al servidor de HackerWatch; éste le registrará y le asignará una identificación de usuario compuesta de cuatro partes, que enviará de vuelta a la dirección de correo previamente facilitada, para después inscribirla en *User ID*.



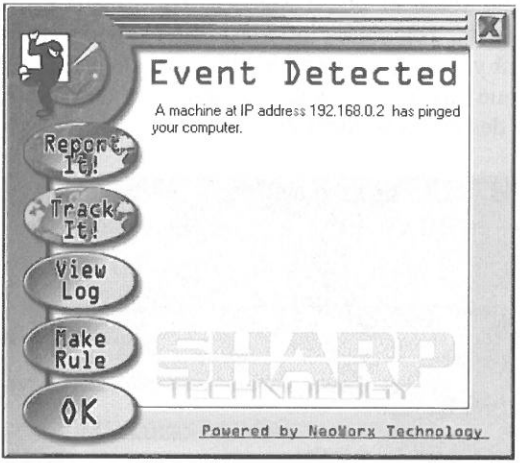
Cuando se haya registrado, el identificador de usuario que le hayan asignado le será enviado a la dirección de correo correspondiente.

6. Importante: una vez inscrita la identificación de usuario, deberá hacer clic de nuevo sobre *OK*. HackTracer aceptará y guardará la identificación de usuario para emplearla automáticamente en futuras notificaciones al servidor de HackerWatch.

Rastrear a los atacantes con HackTracer

Si HackTracer está activo, proporcionará a su PC una protección fiable en función del nivel de seguridad elegido. Además, avisará de cada incidencia de ataque y usted podrá reaccionar en consecuencia. En un recorrido breve le mostraremos las posibilidades de que dispone.

1. Si HackTracer ha registrado un ataque o un acceso contrario a las reglas de seguridad, informará del incidente mediante una ventana de aviso (*Event Detected*). Ésta es visualizada inmediatamente, sin importar las otras aplicaciones que estén siendo ejecutadas en ese momento en el PC. Informará del tipo de ataque y del ordenador desde el que fue lanzado. Además, le facilitará los botones para activar las diferentes medidas que se puedan tomar.



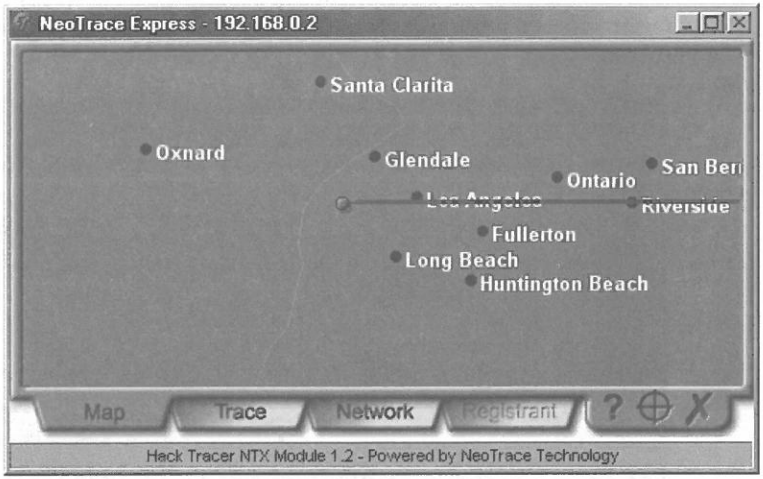
Así notifica HackTracer las incidencias sospechosas.

2. Si el ataque procede de un ordenador desconocido, debería intentar averiguar en primer lugar la identidad de la máquina de origen. Quizá resulte que la causa del aviso fuera inofensiva. Haga clic sobre el botón *Track It!*.

3. A continuación, HackTracer iniciará el módulo gráfico de Traceroute *NeoTrace Express*, una variante aligerada de NeoTrace que ya presentamos anteriormente en este mismo capítulo. Seguirá la conexión desde su PC hasta el ordenador de origen y la representará gráficamente en un mapamundi.

HackTracer representa gráficamente la conexión con el ordenador sospechoso.

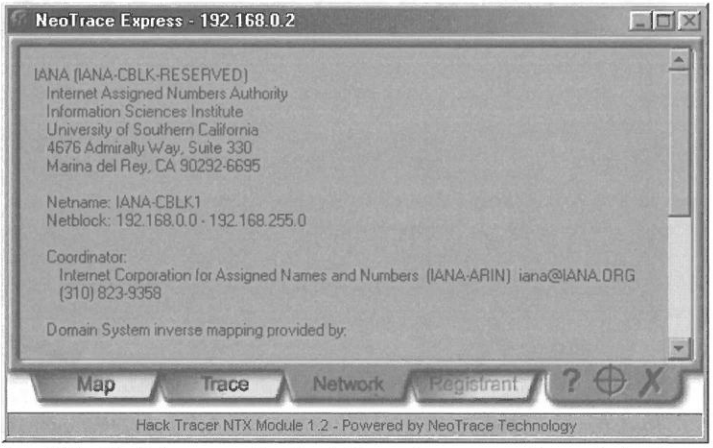
4. Con HackTracer también puede aislar el ordenador de origen sospechoso, ampliando su imagen con una función de zoom. Para eso, haga clic varias veces con el botón izquierdo del mouse sobre la zona próxima al ordenador buscado, hasta que pueda ver los detalles que necesite.



Con la función de zoom se puede cercar al ordenador buscado.

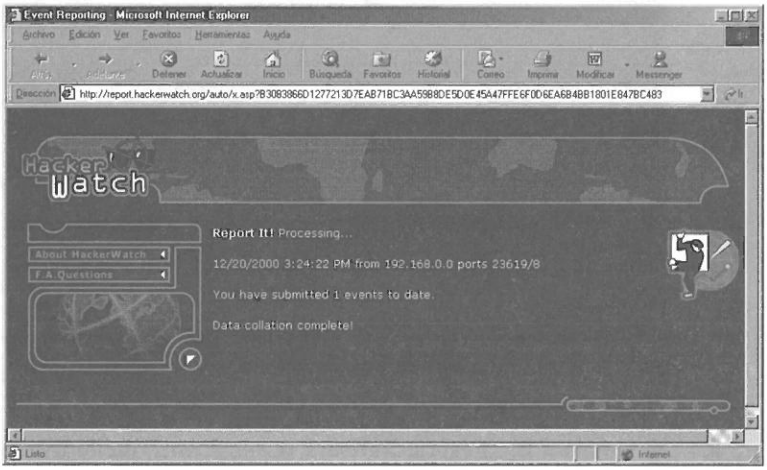
5. Si cambia a la categoría *Network* o *Registrant*, recibirá toda la información disponible sobre ese ordenador en las bases de datos Whois. Así, sabrá quién es el responsable del dominio al que pertenece el ordenador y cómo localizar a la persona de contacto. Cuando haya reunido suficiente infor-

mación, cierre la ventana haciendo clic sobre el símbolo en forma de x situado en la parte inferior derecha.



También HackTracer analiza las informaciones procedentes de las bases de datos Whois.

6. Si usted está convencido de que este acceso ilícito es el ataque de un hacker, podrá notificar el incidente a HackerWatch. Aunque para ello, deberá haberse registrado como usuario según lo descrito anteriormente. Si está registrado, con un simple clic sobre *Report It!* podrá enviar la denuncia del suceso.



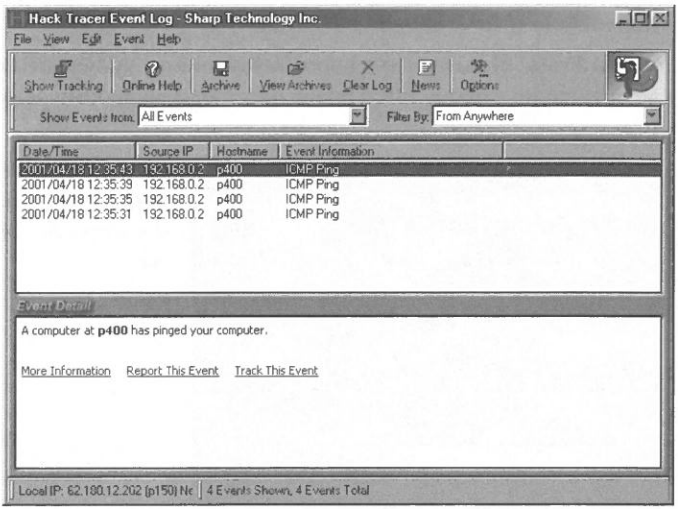
HackTracer arranca el navegador web, para denunciar el ataque al servidor de HackerWatch.

7. Acto seguido, HackTracer genera una denuncia que incluye todos los datos relevantes, como el ordenador de origen, el tipo de ataque y cuándo tuvo lugar. Para enviarla, el programa arrancará el navegador web estándar y mostrará la página de informes del servidor HackerWatch, que recibirá la denuncia y enviará una página de respuesta como acuse de recibo. Si ésta finaliza con el mensaje *Data collation complete*, significará que sus datos han sido recibidos correctamente en el servidor de HackerWatch.

El protocolo de incidencias de HackTracer

Mientras HackTracer no tenga que notificar ninguna incidencia, usted sólo verá del programa un pequeño símbolo situado en la parte inferior derecha de la barra de inicio. Pero también existe un programa principal, que por una parte sirve para la configuración y por la otra, lleva un protocolo de todas las incidencias registradas. Hay dos formas de iniciar este programa:

- Si aparece una ventana de aviso de incidencias, haciendo clic sobre el botón *View Log*, podrá visualizar la ventana principal.
- Aunque no haya habido ninguna incidencia, también puede llamar a la ventana principal haciendo doble clic sobre el símbolo de HackTracer, situado en la parte inferior derecha de la barra de inicio.



En la ventana principal de HackTracer están registradas todas las incidencias.

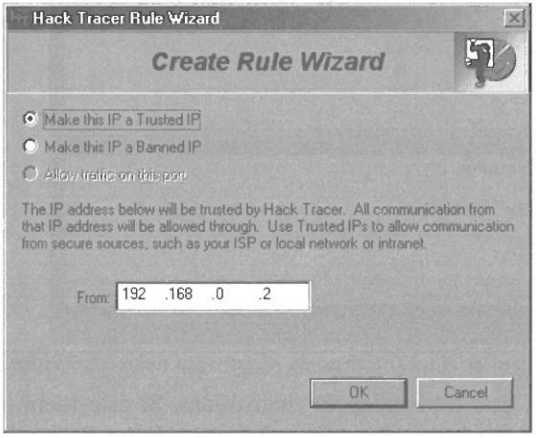
Aquí podrá ver la lista de incidencias registradas. Si ésta fuera muy extensa, podrá recurrir a las funciones *Show Events from* y *Filter By* para que le muestren sólo determinadas incidencias. Si marca una de ellas, aparecerán en la parte inferior *Event Detail* todas las informaciones relacionadas con esa incidencia.

Aquí también encontrará funciones que le permitirán tomar en un momento posterior las medidas que hemos explicado antes. Pero si quiere denunciar una incidencia a HackerWatch, no debería esperar demasiado; habitualmente tienen por norma considerar obsoleto todo lo que tenga una antigüedad mayor de tres días, por lo que ya no lo toman en consideración.

Evitar falsas alarmas

Al principio, quizá compruebe que HackTracer notifica ataques con relativa frecuencia, cuando en realidad se trata de accesos totalmente inofensivos. Esto siempre depende, entre otras cosas, del nivel de seguridad que usted hubiera elegido y de los servicios de Internet empleados. Para evitar que se produzcan con regularidad falsas alarmas, puede definir reglas que decidan los accesos que HackTracer deba permitir sin comentarios.

1. Haga clic sobre el botón *Make Rule*, situado dentro de la ventana de aviso de incidencias. También tiene la alternativa de seleccionar, en cualquier momento posterior, la incidencia en el protocolo y conseguir el mismo efecto con la función de menú *Event/Configure Applicacion Rule on Event*.
2. En ambos casos, usted abrirá *Create Rule Wizard*, un asistente que le ayudará a definir las reglas. Seleccione aquí en primer lugar, si quiere permitir a ese ordenador acceso a nivel general (*Make this IP a Trusted IP*) o si desea impedírselo (*Make this IP a Banned IP*).
3. En el campo *From*: el asistente ya habrá introducido el número IP del ordenador seleccionado. Aunque usted puede hacer aquí las modificaciones que necesite.



Con Create Rule Wizard, puede definir reglas para determinados ordenadores.

4. Si todos los pasos han concluido, guarde la nueva regla haciendo clic sobre el botón *OK*.

A partir de ahora, cualquier intento de contacto por parte de este ordenador será manejado según esta regla. Si ha definido el ordenador como *Trusted IP*, los accesos serán permitidos sin comentarios. Si por el contrario, lo ha proscrito como *Banned IP*, sus accesos serán rechazados también sin comentarios. En cualquier caso, ya no será bombardeado con mensajes de aviso cada vez que ese ordenador intente un acceso. Si más adelante quiere retirar una regla, la encontrará en las configuraciones que podrá abrir con *File/Options*. Éstas incluyen, entre otras, las categorías *Banned IP's* y *Trusted IP's*.

5.3 Recursos legales contra los hackers

Si, después de todo, hemos pillado a un hacker con las manos en la masa, surge la pregunta de hasta qué punto puede ser responsabilizado de sus actos. El pirateo en sí aún no es un crimen. En la mayoría de los casos, el culpable sólo debe esperar consecuencias jurídicas si realmente se han producido daños. En este apartado, vamos a perfilar la persecución por vía penal y por vía civil que podría sufrir un hacker pillado in fraganti. De esta forma, sabrá si tiene algún sentido proceder contra el atacante. Aunque alguna vez abrigue la idea de probar esa u otra herramienta de hacker, debería estudiar este apartado con atención; de este modo, sabrá lo que está permitido y de qué métodos es mejor apartarse.

Persecución por vía penal

Siempre que las acciones de un hacker incurran en delito, se puede presentar una denuncia. Para eso, basta con poner el suceso en conocimiento de la policía o comunicárselo por escrito a la fiscalía. Si hay suficientes puntos de apoyo para hablar de delito, la fiscalía deberá actuar a raíz de esa denuncia. Como denunciante, usted no deberá correr con los gastos de las diligencias. Tampoco será necesario recurrir inmediatamente a un abogado.

Aunque para cometer un delito, un hacker tiene que esforzarse lo suyo. Y es que en términos generales, los intentos no son considerados como punibles. El mejor ejemplo para ilustrar esta afirmación son los portscans. Ejecutarlos y buscar con ellos agujeros de seguridad en el ordenador, es algo completamente legal. Viene a ser como si alguien sacudiera la puerta de un coche aparcado, para comprobar si quizá la han dejado abierta. Esto lo permite la ley sin más. Aunque un hacker aproveche un agujero de seguridad detectado para espiar datos, con esto aún no tendría por qué caer en la ilegalidad. Desde el punto de vista legal, los datos almacenados sin precauciones específicas en un ordenador no están sujetos a ninguna protección especial. Sólo si un hacker espía en un entorno empresarial "secretos comerciales o industriales" por encargo tal vez de la competencia,

podrá hablarse de quebrantamiento de la ley contra competencia desleal. Pero de hecho, esto sólo vale en caso de espionaje económico, no para los ataques a particulares.

Sin embargo, si un hacker – también en un entorno privado – se hace con "datos especialmente protegidos", está cometiendo un delito. Aunque sobre la naturaleza concreta de esta protección especial, seguramente podrían discutir los abogados en el juicio hasta la saciedad. Tal vez las protecciones sencillas como podría ser una contraseña para un documento de Word, no serían suficientes. Encriptando un archivo adicionalmente por medio de un programa especial (por ejemplo PGP), se supone que quedaría expresada con suficiente claridad la intención de protegerlo contra terceros. Por lo tanto, si un hacker fuerza esa encriptación, estará cometiendo un delito.

También se habla definitivamente de delito si el hacker modifica o destruye datos en el ordenador atacado. Aquí no importa si esos datos gozaban de protección específica o no. Aunque ahora, podríamos sostener el criterio de que el mero ataque (por ejemplo con un portscan) ya modifica datos en la memoria de trabajo del ordenador. Pero en la práctica, la interpretación no es tan estricta y se refiere casi exclusivamente a datos o archivos de almacenamiento fijo.

El delito de sabotaje informático

Un aspecto especialmente interesante en relación con los hackers es el delito de sabotaje informático. Esta definición es relativamente amplia y se refiere a todos los daños y perjuicios causados por las actividades de un hacker. Es decir, no sólo incluye daños y manipulaciones reales de archivos, sino quizá ya la interrupción del proceso de datos. Si, por ejemplo, un hacker paraliza un acceso a Internet mediante un ataque Denial of Service o un portscan permanente, ya se puede hablar de sabotaje informático. Aunque en principio, el sabotaje informático sólo puede ser alegado por empresas, autoridades u organizaciones, pero no por particulares. Es decir, el usuario particular aún no tiene la posibilidad de quitarse de encima a un acosador.

Persecución por vía civil

Con independencia del derecho penal, en principio, el ataque de un hacker puede ser perseguido por vía civil, sin importar si constituye un delito o no. Si alguien ha sufrido daños por culpa de un hacker, en principio puede pedir una indemnización por daños y perjuicios. Esto es aplicable si se pueden demostrar de manera concluyente tanto los daños sufridos como el autor de los mismos. Pero las demandas por daños y perjuicios las debe llevar adelante el propio demandante. Es decir, deberá facturar los daños al infractor, reclamar el pago si fuera necesario y, si todo esto no diera resultado, iniciar una acción civil. Naturalmente, con

este procedimiento el demandante se implica mucho. Si pierde la demanda, deberá asumir los gastos judiciales y todos los costes del demandado, sin hablar ya de los propios. Además, en las cuestiones relacionadas con tecnologías novedosas siempre se corre peligro de dar con un juez chapado a la antigua, que no comprenda estas cosas. A pesar de todo, quien haya sufrido daños cuantificables debería consultar a un abogado competente sobre la conveniencia de iniciar una acción civil.

6. Peligros en red – ataques dentro de la red de empresa

6.1 Ataques a PCs integrados en una red **300**
Puertos abiertos – invitaciones para los hackers 301
¿Quién me está espiando? – software para detectar un ataque 309

6.2 Atacar el tráfico de datos dentro de la Red **315**
Fisgoneo de contraseñas y datos confidenciales – Sniffing de paquetes 315

6.3 Vigilancia en el puesto de trabajo – ¿Qué es factible y está permitido? **321**
Posibilidades técnicas para la vigilancia 322
¿Justicia ante todo? – esto es lo que el jefe tiene derecho a saber sobre usted 322
Las reglas de oro – así debe actuar 325

6.4 Borrar las huellas delatoras de su navegación por Internet **326**
Borrar el caché y los datos de historial del navegador 327
Proteger las contraseñas privadas en el puesto de trabajo 338
Datos privados confidenciales en el puesto de trabajo 342

6.5 Windows en la red: una combinación peligrosa **345**
El uso compartido de archivos e impresoras 345
Los protocolos de red: una fuente de peligros 354
El Servidor de acceso telefónico a redes como vía de invasión 359

En los capítulos precedentes, nos hemos ocupado de ordenadores Windows independientes, que a lo sumo pueden ser enlazados con la red mediante una conexión telefónica vía módem o un adaptador RDSI. Pero no sólo en las empresas grandes se están imponiendo las redes. También los usuarios particulares y los despachos pequeños están obteniendo más y más provecho de la ventaja que ofrece la interconexión de ordenadores independientes en una red. Esto se debe sobre todo al hecho de que los costes de una interconexión en red han bajado mucho. Por menos de 35.000 pesetas, ya se pueden adquirir paquetes básicos de red con dos tarjetas de red y cables para la conexión de dos PC. También redes de mayor envergadura, desde 3 a 100 PCs o más, pueden comprarse a un coste razonable.

La interconexión en red también trae consigo peligros. Por una parte, el intercambio libre de datos puede convertirse en un bumerang. Si un virus ha penetrado en un ordenador de la red, conquistar toda la red es un juego de niños para él. Y, desgraciadamente, la situación es parecida en los ataques de hackers. Si un hacker ha logrado acceder a un ordenador, desde allí será mucho más sencillo atacar a otros componentes de la red. Sobre todo si las medidas de seguridad se aplican con laxitud. Si además una red ofrece acceso a Internet para los ordenadores conectados, se les abrirá a los atacantes una regia vía para penetrar desde una distancia segura en la red de una empresa y, de este modo, en los ordenadores conectados.

Pero no siempre los atacantes vienen de fuera. Una red de empresa también ofrece a los "encantadores" colegas amplias posibilidades para espiar a sus compañeros de trabajo o incluso sabotearles, ya sea de "broma" o con mala intención. Donde en otras circunstancias había que reventar la puerta de una oficina o el cajón de un escritorio, gracias a los vínculos de red entre todos los ordenadores bastan unas nociones básicas sobre agujeros de seguridad o configuraciones incorrectas. En este capítulo vamos a mostrarle cómo evitar estas trampas para proteger eficazmente en un entorno de redes tanto los datos de la empresa como los particulares.

6.1 Ataques a PCs integrados en una red

En principio, los PCs integrados en una red pueden ser atacados del mismo modo que los ordenadores que enlazan con Internet por una conexión telefónica vía módem o un adaptador RDSI. Se trata sólo de dos métodos diferentes para obtener el mismo resultado, es decir, una conexión de red con otros ordenadores. A pesar de todo, los PCs con conexión de red fija están expuestos a un peligro mucho mayor, aunque sólo sea por el hecho de que un PC conectado a una red puede ser atacado a todas horas o, al menos, todo el tiempo que dure la conexión. Un PC con conexión telefónica que sólo entre en Internet media hora al día, únicamente podrá ser atacado durante esa media hora, si bien esa media hora ya bastaría para un ataque selectivo. Pero muchos hackers primero lanzan sus ataques al buen tuntún, según el lema "¿Qué ordenadores tengo a mi alcance para atacar?". Naturalmente, en este caso un PC permanentemente conectado a la Red está mucho más amenazado. A esto habría que añadir que una conexión directa a la Red suele ser bastante más potente que una conexión telefónica por módem o RDSI, de modo que el tráfico de datos adicional provocado por un ataque no llamaría la atención y el usuario casi nunca se percataría de él. Con una conexión telefónica de banda estrecha, si un rendimiento habitualmente bueno desciende de pronto bajo mínimos, el usuario seguramente sospecharía que algo raro está ocurriendo.

TRUCO

Conexión a la red frente a tarifa plana ADSL

Últimamente, en el ámbito de la conexión a Internet están adquiriendo cada vez mayor importancia dos técnicas nuevas: con el procedimiento de enlace asíncrono ADSL se puede alcanzar en conexiones telefónicas convencionales una velocidad de datos mucho mayor. La tarifa plana permite a los usuarios de Internet conectarse las 24 horas del día a un precio fijo. La combinación de ambas técnicas, ADSL y tarifa plana, plantearía cuestiones importantes en relación con la seguridad. Un PC con acceso DSL alcanza velocidades de datos absolutamente equiparables a las de una conexión de red directa. Además, si con la tarifa plana está conectado regularmente a Internet durante muchas horas, casi se pondría al nivel de un PC con conexión a la red, cosa que está muy bien para el internauta, pero éste debería ser consciente de que así, su PC queda expuesto a los mismos peligros que un ordenador integrado en una red. Es decir, también podrá ser atacado en cualquier momento desde el exterior, por lo que debería protegerlo en consecuencia.

Puertos abiertos – invitaciones para los hackers

Cuando un hacker intenta atacar a un ordenador integrado en una red, su primer recurso suele ser un portscan (escaneado de puertos). Casi siempre, éste ya le revela todo lo que necesita saber sobre el ordenador y, en consecuencia, para la planificación ulterior de su ataque. ¿Qué es exactamente un portscan? Cuando un PC está conectado a Internet, puede intercambiar datos con otros ordenadores de la Red a través del protocolo TCP/IP. Como sin duda ya sabrá, Internet se compone de una amplia serie de servicios. Tenemos por ejemplo el correo electrónico, la web, los grupos de noticias, las descargas de archivos, los chats, etc. Cada uno de estos servicios emplea sus propios protocolos que, sin embargo, se basan todos en El Protocolo, con mayúsculas, de Internet: TCP/IP. Para que con tantos servicios y protocolos no haya confusiones, la comunicación de datos dentro de Internet va subdividida en varias secciones. Tenemos por ejemplo una sección para solicitar y transmitir páginas web, una para intercambiar mensajes de correo electrónico, etc. Si un ordenador de Internet quiere utilizar estos servicios, deberá establecer un vínculo con la sección correspondiente. Este vínculo recibe el nombre de Puerto. Para todos los servicios estándar importantes hay puertos estándar fijos, como por ejemplo el puerto 80 para la Red. Pero aparte de estos, hay también varios miles de puertos al alcance de todo el mundo que pueden ser usados, por ejemplo, por cualquier programa de Internet.

Mediante un portscan, un hacker puede averiguar los servicios de Internet que utiliza u ofrece su PC. Para eso, simplemente envía una consulta a un puerto y espera a ver si le llega una respuesta. Si, por ejemplo, envía una consulta al puerto 20 y recibe una respuesta, sabrá que en su PC trabaja un servidor FTP, ya que el puerto 20 (y el 21) son los responsables del servicio de transmisión de datos FTP. Con estos conocimientos, el agresor podría intentar acceder a su ordenador

a través del servidor FTP. Aplicando este principio, los hackers pueden explorar su PC sistemáticamente, por el sencillo procedimiento de enviar consultas a todos los puertos imaginables y evaluar después la reacción. Así, en muy poco tiempo saben las conexiones que soporta su ordenador y pueden planificar cómo seguir con el ataque.

INFO

¿Son legales los portscans?

Hasta la fecha, un portscan es absolutamente legal. La comprobación de un puerto es una posibilidad totalmente regular de TCP/IP y, desde el punto de vista técnico, no supone de ningún modo un pirateo. Tampoco se considera un delito penal testear sistemáticamente muchos o todos los puertos de un ordenador. Esto es como si usted andara por la calle y en todos los coches aparcados, accionara brevemente el tirador de la puerta para ver si encontraba algún vehículo abierto. Sólo si realmente abre la puerta, se sienta dentro y hace el puente en el encendido, cometerá un delito. Lo mismo sucede con los portscans. Sólo si usted aprovecha los resultados de un escaneo para procurarse acceso y manipular o destruir datos, cometerá un delito. Hasta entonces, únicamente se hablará de juegos técnicos. En el último apartado del capítulo 5 puede encontrar más información sobre cuestiones legales.

Comprobar el ordenador mediante portscans

Ahora queremos enseñarle cómo realizar usted mismo un portscan. Naturalmente, con esto no pretendemos darle instrucciones para infiltrarse en los ordenadores de otros usuarios. Más bien queremos que pruebe a penetrar en su propio PC. Este ataque simulado no causará ningún daño, pero usted podrá detectar los fallos de seguridad de su propio PC y ver la facilidad o dificultad para aprovecharlos y proporcionarse acceso a datos importantes. En este ejemplo utilizaremos el portscanner Yet another Portscanner YAPS. Encontrarán una versión de prueba gratuita de este programa en http://www.tni.net/~ted/Yaps/Yaps.html.

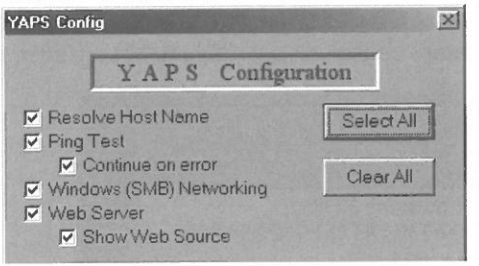
Hay una gran variedad de portscanners, pero nosotros hemos elegido éste porque no se limita a escanear simplemente los puertos, sino que también ayuda al usuario a la hora de evaluar los resultados. Así, YAPS busca automáticamente algunos agujeros de seguridad y configuraciones incorrectas más frecuentes. Si se supera una pasada completa de prueba con este programa sin haber recibido ningún mensaje dramático, se podrá suponer que el PC está bastante seguro. De recibirse mensajes, se podrá averiguar la causa y mejorar la seguridad.

Configurar YAPS para el portscan

Antes de emplear YAPS para un portscan, debería verificar primero la configuración del programa. Éste puede ser configurado con gran exactitud mediante una gran cantidad de opciones y ajustes. Esto permite, por un lado, ejecutar un scan muy completo, que por cierto requiere su tiempo. Por otra parte, también se pueden hacer tests muy específicos de los diferentes puertos o de determinados agujeros de seguridad, con los que enseguida se obtienen resultados.

1. Para ver y modificar la configuración de YAPS, arranque el programa (normalmente con *Inicio/Programas/YAPS/YAPS*) y, en la ventana principal, haga clic sobre el botón *Configure*.

2. Así abrirá el cuadro de diálogo *YAPS Config*, donde podrá realizar de modo centralizado todos los ajustes de YAPS. En la parte derecha encontrará dos botones para activar todas las opciones (*Select All*) o desactivarlas (*Clear All*).



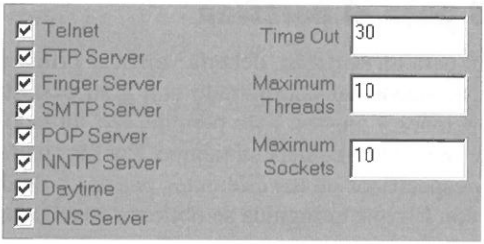
En el cuadro de diálogo de configuración de YAPS puede seleccionar los diferentes tests que quiere ejecutar.

3. Con la opción *Resolve Host Name*, los números IP de los ordenadores de Internet que se vayan a verificar son descompuestos en los correspondientes nombres IP. Esto es útil si usted no conoce el o los nombres. De lo contrario, debería desactivar esta opción, ya que en determinadas circunstancias puede llevar mucho tiempo.

4. *Ping Test* verifica lo que dura la transmisión de datos al ordenador escaneado e indica la duración más corta, la más larga y la media. Si usted activa además la opción *Continue on error*, los tests continuarán aunque algunos pings no reciban respuesta.

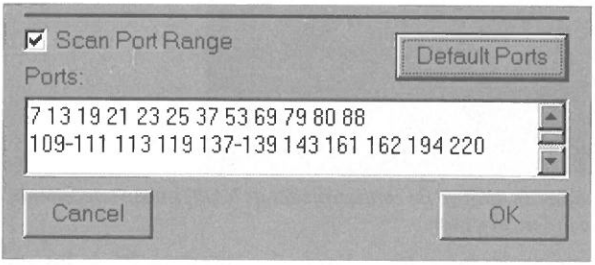
5. Cuando se comprueben ordenadores con Windows, es muy importante activar la opción *Windows (SMB) Networking*. Busca en el PC escaneado las impresoras y los archivos compartidos.

6. Active la opción *Web Server* para escanear en busca de un servidor web en el ordenador a verificar. Si además está activada la opción *Show Web Source*, YAPS llamará automáticamente a la página inicial del servidor web.



Estas opciones le permiten a usted escanear en busca de los servicios de Internet más importantes.

7. Debajo hay una serie de opciones con las que usted puede realizar tests en busca de los servicios de Internet más importantes. Para cada opción activada, YAPS realiza un portscan y, si encuentra el servicio correspondiente, lo reflejará en el resultado de scan. Las configuraciones en la parte superior derecha indican la cantidad máxima de conexiones paralelas que YAPS puede establecer para el test. En la versión de prueba vienen limitadas, por lo que le recomendamos conservar la configuración estándar.



Con Scan Port Range puede escanear los puertos que quiera.

8. Si aparte del test estándar desea realizar más portscans, active la opción *Scan Port Range*. Después podrá indicar en el campo *Ports* los puertos que quiera testear. Hay que separar los diferentes números de puerto con un carácter en blanco. Si usted teclea un guión entre dos números de puerto, será interpretado como un intervalo y se testearán todos los puertos que haya en el intervalo.

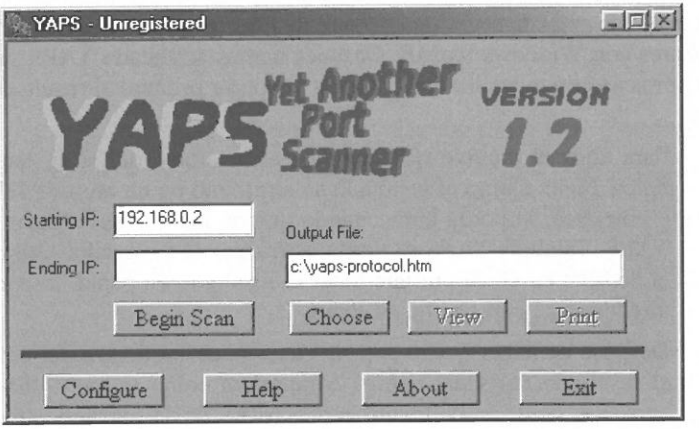
9. Haciendo clic en el botón *Default Ports*, incluirá en el campo de entrada una serie de puertos estándar e intervalos de puerto predefinidos que, según ha demostrado la experiencia, arrojan los resultados más interesantes.

10. Guarde las configuraciones de portscan haciendo clic en *OK*.

Realizar el portscan

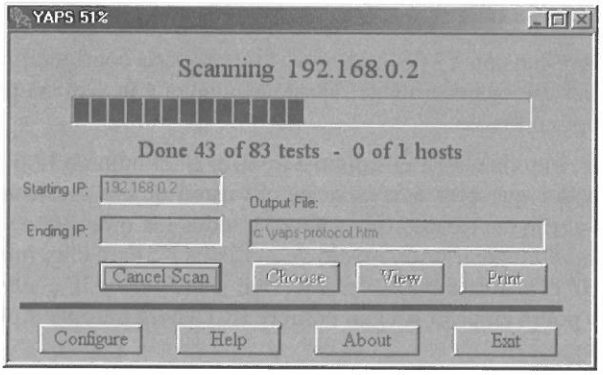
Para realizar un portscan con YAPS, en primer lugar debería configurar la herramienta según lo descrito anteriormente. Después, vuelva a la ventana principal para iniciar el propio portscan.

1. Para empezar, introduzca en el campo *Starting IP* el número IP o nombre IP del ordenador que pretenda escanear. Si usted quiere escanear varios ordenadores al mismo tiempo (por ejemplo, todos los ordenadores de una red local), podrá emplear un intervalo de números IP. Para ello, introduzca en *Starting IP* el primer número del intervalo y en *Ending IP* el último. En este caso, no podrá emplear ningún nombre IP. Deberá introducir obligatoriamente números IP.
2. A continuación, introduzca en el campo *Output File* el archivo donde deba ser guardado el resultado del portscan. YAPS genera un archivo en formato HTML que después puede ser visualizado con cualquier navegador web. Si quiere crear un archivo nuevo, basta con que introduzca en el campo una nueva ruta y un nuevo nombre de archivo. Si lo que desea es sobrescribir un archivo ya existente, con *Choose* podrá abrir un cuadro de diálogo para seleccionar el archivo.
3. Con esto habrá concluido todos los preparativos y podrá iniciar el portscan con un clic en *Begin Scan*.



YAPS ya está configurado y puede iniciar el portscan.

4. Ahora, YAPS realizará por orden los escaneos establecidos en la configuración. La información obtenida se reflejará en el archivo de resultados elegido. Mientras tanto, una ventana de estado le mantendrá al corriente y le informará de los progresos obtenidos.



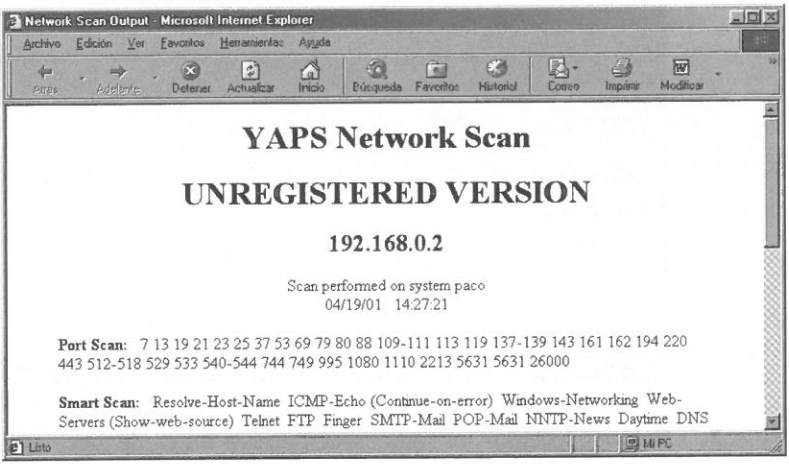
Durante el portscan en ejecución, YAPS le informa de los progresos.

Al concluir, YAPS regresa a la ventana principal de costumbre. Podrá comprobar que se realizó el portscan, porque ahora estarán activados los botones *View* y *Print*, que permiten ver e imprimir el resultado del scan.

Evaluar los resultados

Una vez realizado el portscan, puede ver el resultado de las pruebas y analizar qué estado posee el ordenador escaneado y qué agujeros de seguridad podrían derivarse de este. Para el siguiente ejemplo, hemos preparado un ordenador con algunos agujeros de seguridad típicos, de los que se dan con frecuencia en ordenadores con Windows 9x/ME. Después hemos arrancado YAPS para que haga un portscan con todos los tests. Vamos a repasar primero el resultado de la prueba:

1. Para abrir el archivo que contiene el resultado del scan, haga clic en el botón *View*. Como el resultado se almacenó en un archivo HTML normal y corriente, lo podrá abrir cuando quiera, incluso sin utilizar el programa YAPS. También YAPS se limita a arrancar el navegador estándar y a abrir el archivo en él. Si prefiere tener el resultado en papel, lo podrá imprimir directamente con un clic en *Print*.
2. Después de haber hecho clic en *View*, se abrirá dentro del navegador web el resultado del scan, que se comportará como si fuera una página web corriente. Es decir, podrá utilizar las barras de desplazamiento para recorrer el documento hacia arriba o hacia abajo.
3. Al principio encontrará un resumen de la configuración. En él figuran el ordenador verificado y el momento en que se realizó el portscan. Debajo vienen los puertos analizados y los *smartscans* realizados, es decir, los tests específicos en busca de determinados agujeros de seguridad.

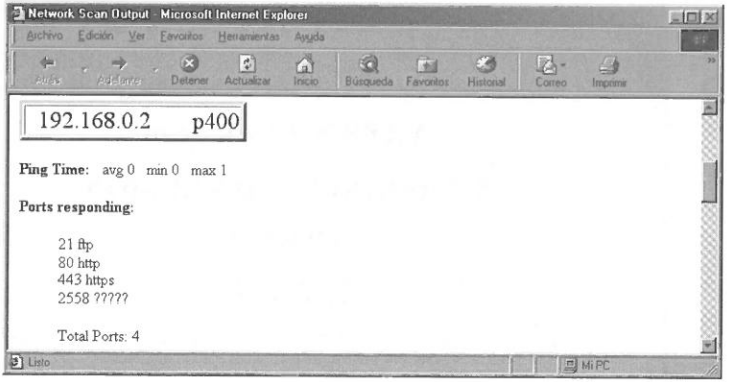


Arriba se resume la configuración con la que se realizó el portscan.

4. Debajo vienen los verdaderos resultados del scan. Primero figura el número IP del ordenador escaneado. Si YAPS pudo averiguar el correspondiente nombre IP, también lo mostrará.

5. A continuación viene el resultado de los pings. Se indica el tiempo medio (*avg*), el más corto (*min*) y el más largo (*max*) que hubo que esperar. En nuestro ejemplo, el ordenador escaneado se encontraba muy próximo, de modo que la conexión fue muy rápida. Así que el *0* no significa que no hubiera respuesta al ping, sino que ésta se produjo sin un retraso perceptible.

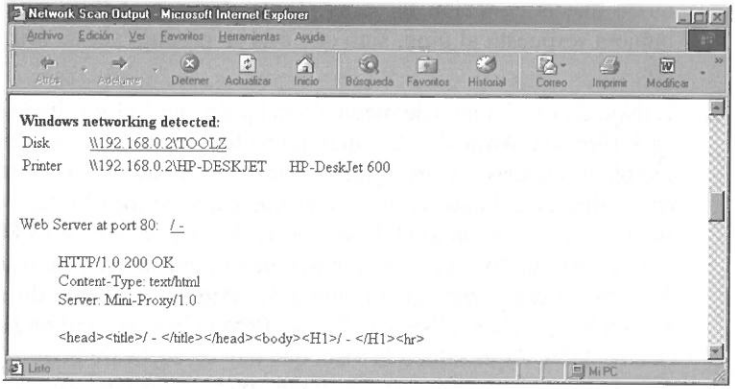
6. Debajo de los tiempos de medición del ping viene el resultado de los portscans directos. Aquí YAPS indica todos los puertos escaneados de los que recibiera respuesta. Esto significa que en esos puertos existe la posibilidad de establecer comunicación con el ordenador verificado. En nuestro ejemplo el scan reveló un total de 4 puertos abiertos. Los puertos 80 y 443 pueden ser atribuidos a un servidor web que trabaja en el ordenador. El puerto 21 está ocupado por un servidor FTP. Ambos servicios de servidor son sometidos a más análisis detallados. Pero debemos fijarnos sin falta en el puerto 2558. Aquí salta a la vista que hay un software activo que opera en ese puerto. Como no se trata de ningún puerto estándar, esto podría ser indicio de la existencia de un troyano activo que puede ser controlado a través del puerto.



En el protocolo de YAPS figuran todos los puertos que han reaccionado al scan.

7. Después tenemos los tests específicos en busca de agujeros de seguridad concretos. En nuestro ejemplo, YAPS ha detectado en el ordenador escaneado un uso compartido de archivos e impresoras. El de archivos ni siquiera va protegido por contraseña, de modo que haciendo clic en el enlace abriríamos directamente el acceso a las carpetas.

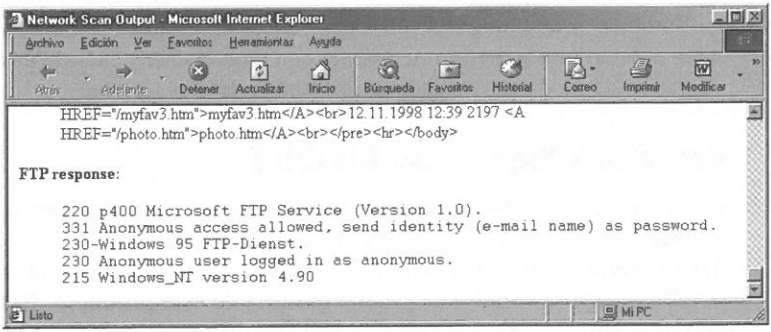
8. Además, YAPS ha detectado en el puerto 80 un servidor de web activo. Desde allí llama inmediatamente al documento de arranque y recoge el correspondiente texto fuente HTML en el resultado.



YAPS ha detectado un uso compartido de archivos e impresoras, así como un servidor web en funcionamiento.

9. Para concluir, viene la comprobación del puerto FTP. Aquí YAPS ha detectado un servidor FTP en activo. En estos casos, el programa intenta automáticamente conseguir acceso anónimo a través de FTP. Como puede verse en el resultado, el intento tuvo éxito. Es decir, sin indicar ninguna contra-

seña, se puede acceder a los archivos del ordenador escaneado. Este agujero de seguridad suele ser a menudo resultado de una configuración incorrecta. Y, con frecuencia, el usuario del PC no sabe nada del servidor FTP ni del acceso anónimo.



Especialmente grave: también existe un servidor FTP que permite un acceso anónimo.

Los conocimientos obtenidos con el portscan permiten sacar conclusiones sobre los posibles métodos de ataque que pudieran tener éxito en este ordenador. En el capítulo 1 ya hemos expuesto en detalle el modo de proceder de los hackers y sus formas de atacar. Allí también puede encontrar información sobre los diferentes ataques con los que es posible aprovechar los agujeros de seguridad descritos.

¿Quién me está espiando? – software para detectar un ataque

¿Cómo nos podemos proteger de los portscans? Obviamente, la solución más radical sería desconectar el ordenador de la red. Pero esto no tiene ningún sentido, por lo que esa desconexión debe hacerse virtualmente, por ejemplo, desactivando todos los servicios que no sean estrictamente necesarios. ¿Por qué debe operar en el ordenador un servidor web o un servidor FTP, por poner dos ejemplos, si no hacen ninguna falta? Si queremos ofrecer determinados servicios de servidor, tendremos que activarlos. Una protección bastante buena contra los portscans y los ataques que puedan traer consigo, la ofrecen los firewalls personales que hemos explicado en el capítulo 4. Bloquean todos los puertos que no sean esenciales y los ocultan de los portscans. De este modo, el atacante se queda en la ignorancia. Aunque lo mismo le ocurrirá a usted. Pese a que algunos firewalls ofrecen funciones de resultados donde recogen, por ejemplo, los intentos de acceder a puertos bloqueados, después resulta laborioso o incluso imposible saber si sólo se trataba de un paquete de datos extraviado o de un ataque en serio.

Para que el ataque sea repelido en silencio y usted sea informado inmediatamente sobre el mismo, existe un tipo especial de software llamado *Intrusion Detection Systems IDS* (en español: sistemas de detección de ataques). Se trata de programas especiales que vigilan el tráfico de datos, de modo similar a lo que hacen los firewalls. Pero no se limitan a bloquear los intentos de contacto ilícito. También procuran hallar en ellos pautas de ataques selectivos. Así, podrá saber cuándo está sometido su ordenador a un portscan y cuándo un atacante está buscando de modo muy selectivo los puntos débiles típicos.

Detectar ataques con BlackICE

Un sistema de detección de ataques de este tipo enfocado a Windows 9X/ME es *BlackICE*, que puede adquirir por unas 6.500 pesetas en *http://www.networkice.com*. Por desgracia, en estos momentos no hay disponible ninguna versión de prueba gratuita de este producto. BlackICE es el complemento óptimo para un firewall flexible, ya que este último está especializado en detectar los ataques y sólo puede bloquear el flujo de datos siguiendo criterios muy toscos, pero es a todas luces incapaz de filtrar con la flexibilidad de un potente firewall.

1. Una vez instalado BlackICE aparecerá en la parte inferior de la pantalla, concretamente en la bandeja del sistema, el icono que representa al programa activo. En el futuro, este será activado automáticamente con cada arranque del sistema, salvo que usted lo desactive expresamente. Haciendo doble clic en el símbolo, también se puede acceder al programa de administración.

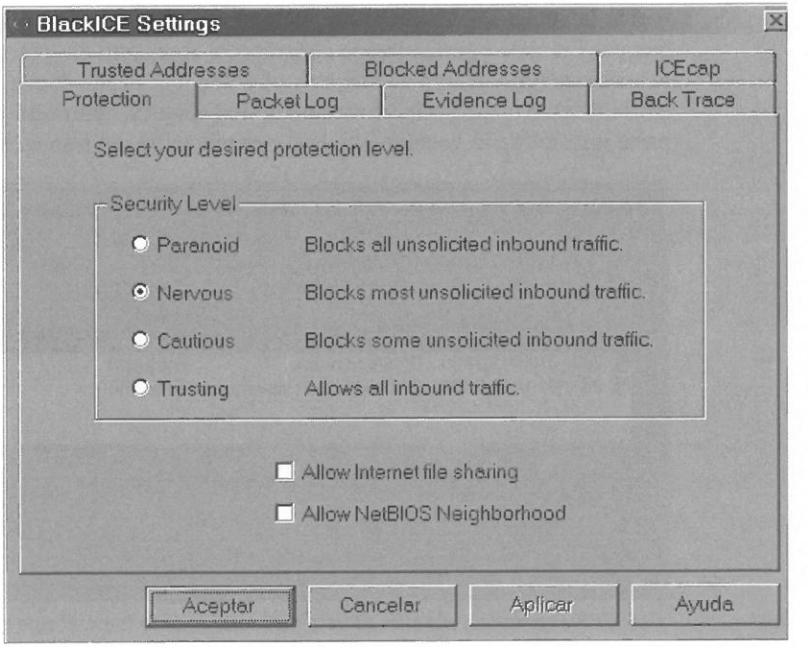
Podrá saber si BlackICE está activado por el icono que aparece en la bandeja del sistema.

2. Para poder confiar en el programa, debería seleccionar en primer lugar el nivel de seguridad deseado. Desde el programa de administración, abra con *Tools/Edit BlackICE Settings* el cuadro de diálogo de configuración y pulse sobre la pestaña Protection.

3. Ahora podrá seleccionar el nivel de seguridad deseado en el área *Security Level:*

   - *Paranoid* impide todo tráfico de datos de entrada. Con esta opción no se puede realizar ninguna función de Internet. Esta configuración sólo puede tener sentido provisionalmente.
   - *Nervous* es la más estricta de las dos configuraciones razonables. Impide la mayor parte del tráfico de datos de entrada, pero seguirá permitiendo las transmisiones que usted mismo inicie, como pueden ser las páginas web solicitadas. En principio, esta configuración es recomendable.

- *Cautious* es algo menos estricto que *Nervous* y bloquea sólo los datos de entrada que sean considerados como peligrosos. Le recomendamos elegir este ajuste sólo si el mayor rigor de *Nervous* le causa problemas con determinadas aplicaciones.
- Con la configuración *Trusting* puede demostrar una gran confianza y permitir el paso de todo tipo de datos que lleguen. Esto no resulta demasiado seguro, pero puede ser una configuración conveniente si su sistema ya está protegido por un firewall personal.



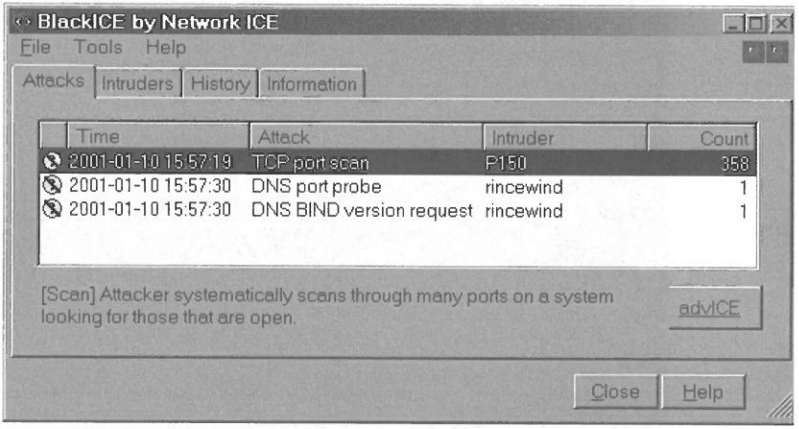
Seleccione el nivel de seguridad que deba establecer BlackICE para su PC.

4. Activando las dos opciones inferiores permitirá que su PC comparta archivos con otros ordenadores a través de Internet (*Allow Internet file sharing*) y que su PC y los recursos de éste aparezcan en el entorno de red de la red local (*Allow NetBIOS Neighbourhood*).
5. Guarde con Aceptar las opciones que haya modificado.

Reaccionar ante las alarmas de BlackICE

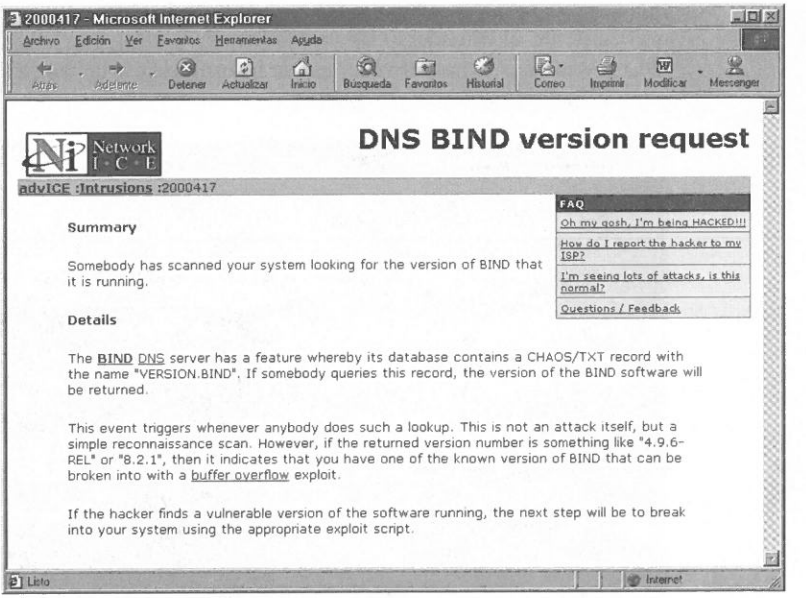
Ahora, BlackICE actuará automáticamente según la configuración seleccionada. Normalmente lo hará con discreción en segundo plano. Si el programa detecta actividades que considere amenazantes, empezará a parpadear el icono de la bandeja del sistema. Como complemento, puede configurar en *Tools/Preferences* una alarma acústica.

1. En caso de alarma, bastará con hacer clic en el icono parpadeante de BlackICE para abrir la ventana principal. En esta aparecerá automáticamente la categoría *Attacks*, que incluye una lista de todos los intentos de ataque. En cada entrada puede consultar el momento en que se produjo el supuesto ataque, el tipo de ataque y el ordenador desde donde partieron las actividades. Si usted selecciona uno de los ataques, aparecerá además en la parte inferior de la ventana una breve explicación del tipo de agresión.



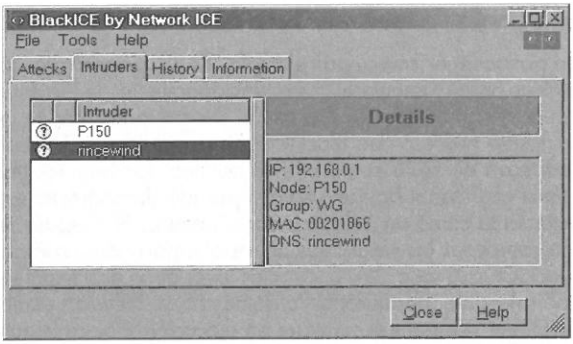
BlackICE registra los ataques detectados mostrando la hora, el tipo y el origen.

2. Si selecciona un ataque y hace clic sobre el botón *advICE*, situado en la parte inferior derecha, podrá solicitar on-line una explicación detallada del ataque en la página web del fabricante de BlackICE.



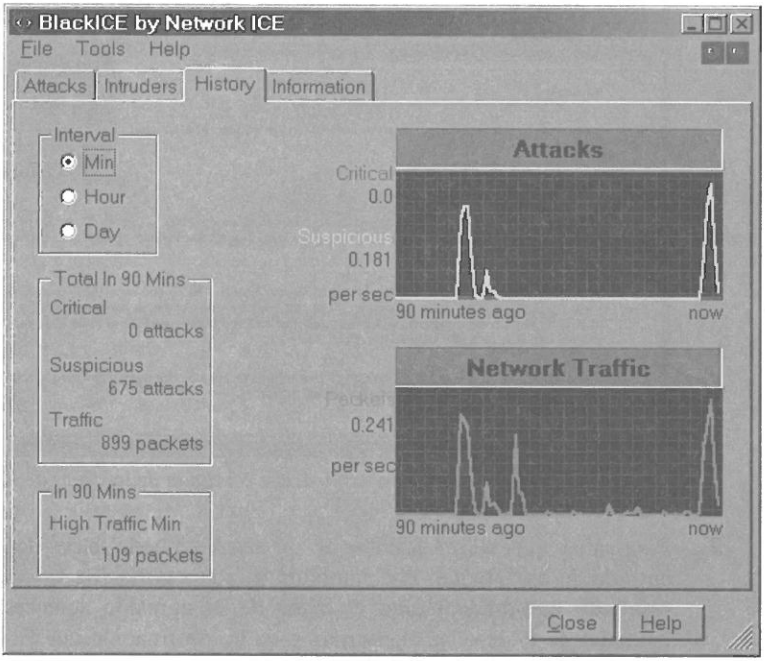
Se puede solicitar on-line una explicación detallada de los tipos de ataque, que además incluye consejos.

3. Para saber más sobre el autor de un ataque, puede hacer doble clic en la entrada de ese ataque. Así cambiará a la categoría *Intruders*, donde será resaltado automáticamente el autor de la agresión seleccionada. En el recuadro de la derecha encontrará toda la información que BlackICE pudo reunir sobre ese ordenador. Estos datos pueden servir como punto de partida para la investigación, según hemos descrito en el capítulo 5.



En la categoría Intruders encontrará información sobre el ordenador del que partió el ataque.

4. Finalmente, también tiene interés la categoría *History*, donde se representa gráficamente el transcurso de un ataque. Para ello, BlackICE recopila los datos esenciales, como el volumen de información y la cantidad de ataques, y los visualiza mediante un gráfico.



La categoría History muestra el transcurso de un ataque a lo largo de un determinado periodo de tiempo.

TRUCO

Haga usted la prueba

Usando un portscanner como, por ejemplo, YAPS, presentado más arriba, puede verificar perfectamente el buen funcionamiento de BlackICE. ¿Por qué no hace un portscan sin BlackICE o con él desactivado y repite después exactamente el mismo proceso con BlackICE? Verá que BlackICE reconoce debidamente el portscan de YAPS como tal y lo notifica. También los tests especiales de YAPS para verificar si hay un uso compartido de archivos, son reconocidos correctamente como un peligro y comunicados. Si después se toma la molestia de comparar los resultados de los dos portscans, comprobará que estando BlackICE activado, YAPS no pudo averiguar prácticamente ninguna información relevante, aunque por lo demás no se hicieran cambios en la configuración del PC ni en el software en ejecución. Por consiguiente, BlackICE impide eficazmente los portscans, mostrando al atacante un sistema completamente hermético. Al mismo tiempo, le avisará del ataque y podrá tomar sus contramedidas.

6.2 Atacar el tráfico de datos dentro de la r

En el capítulo 1 hemos expuesto una amplia serie de diferentes ataqu
hackers. Prácticamente todos estos ataques pueden ser ejecutados tambi
conectados a una red . Sin embargo, la técnica de redes hace que exist
método de ataque especiales que no pueden realizarse sin conexión a la

Fisgoneo de contraseñas y datos confidenciale

Sniffing de paquetes

Un peligro especialmente grande dentro de una red es el "sniffing" de paqu
también llamado simplemente sniffing. Esta expresión describe una técnica
permite interceptar el tráfico de datos en ordenadores vecinos, aunque este
vaya dirigido al ordenador del fisgón. Hay software especial con el que se p
den pinchar los paquetes de datos y registrarlos. Estos programas posibilitan
grabación de los paquetes de datos procedentes de la red para reconstruir de
pués la comunicación que ha tenido lugar.

INFO

Tarjetas de red parlanchinas

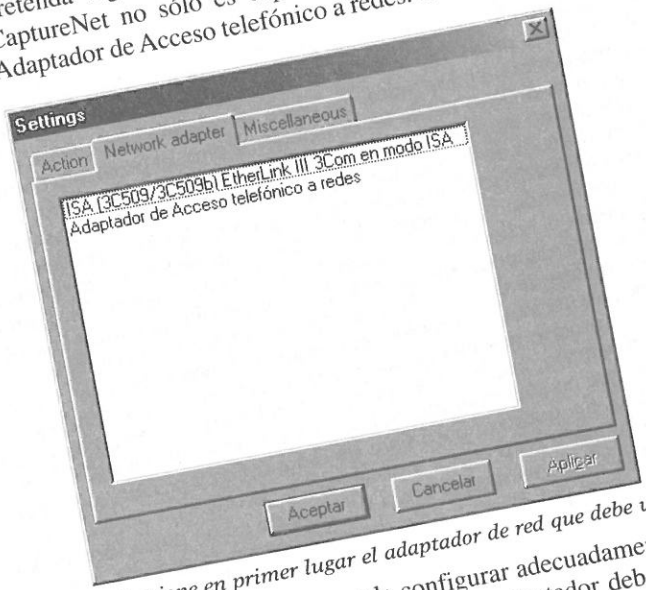
Para comprender cómo funciona el sniffing, se necesitan algunas nociones básicas sobre redes. No tema, que vamos a intentar explicarlo del modo más indoloro posible. En las redes, los datos se envían en paquetes. Si usted transmite un archivo desde un ordenador a otro, el protocolo de red lo descompondrá en muchos bloques de datos pequeños, que enviará independientemente a través de la red. Esto aumenta la eficacia de la transmisión, ya que en caso de perderse datos, sólo habrá que reenviar los paquetes que se hayan extraviado. En principio, los paquetes de datos son enviados directamente desde el ordenador remitente al ordenador receptor. Pero, en la práctica, no todo ordenador está conectado directamente con cada una de las otras máquinas de una red. En ese caso, los paquetes son remitidos por los ordenadores vecinos al receptor real. Aquí es donde entran en acción los sniffers. El usuario que esté sentado ante uno de los ordenadores que participen en el reenvío, puede hacer trabajar a la tarjeta de red en un modo especial en el que no sólo transmite datos, sino que también los lee. Este modo, en realidad, fue pensado para fines de diagnóstico y prueba, pero puede ser usado ilícitamente para espiar todo el tráfico de datos de un ordenador contiguo. Emplazando un ataque espía de este tipo en un punto tácticamente favorable, como por ejemplo un ordenador central de servidor o de interconexión, se podrá interceptar casi todo el tráfico en la red.

gilancia de la red con SpyNet

n sniffer de paquetes de este tipo para Windows es *SpyNet*. Para ser exactos, s una combinación de los programas *CaptureNet* y *PeepNet*. CaptureNet es el rograma sniffer en sí, que espía el tráfico en la red y guarda los paquetes de datos. PeepNet es un programa para analizar los datos recopilados por CaptureNet. Utilizando los paquetes de datos guardados, puede reconstruir la comunicación y visualizar así, por ejemplo, los mensajes de correo enviados o las páginas web visitadas. Puede encontrar una versión gratuita del programa en http://packetstorm.securify.com/sniffers/spynet/.

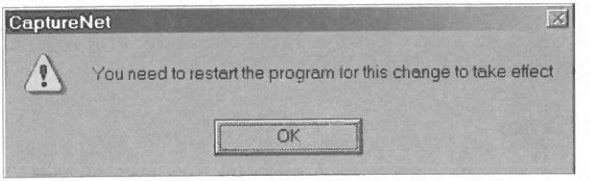
Configurar y activar CaptureNet

1. Para espiar el tráfico de datos, arranque CaptureNet tras su instalación con *Inicio/Programas/SpyNet/CaptureNet*. En el primer arranque se abrirá automáticamente el cuadro de diálogo de configuración mostrando la pestaña *Network adapter*. Aquí deberá seleccionar el adaptador de red que pretenda vigilar. En la lista aparecen todos los adaptadores instalados. CaptureNet no sólo es capaz de espiar tarjetas de red, sino también el Adaptador de Acceso telefónico a redes. Confirme su elección con *Aceptar*.



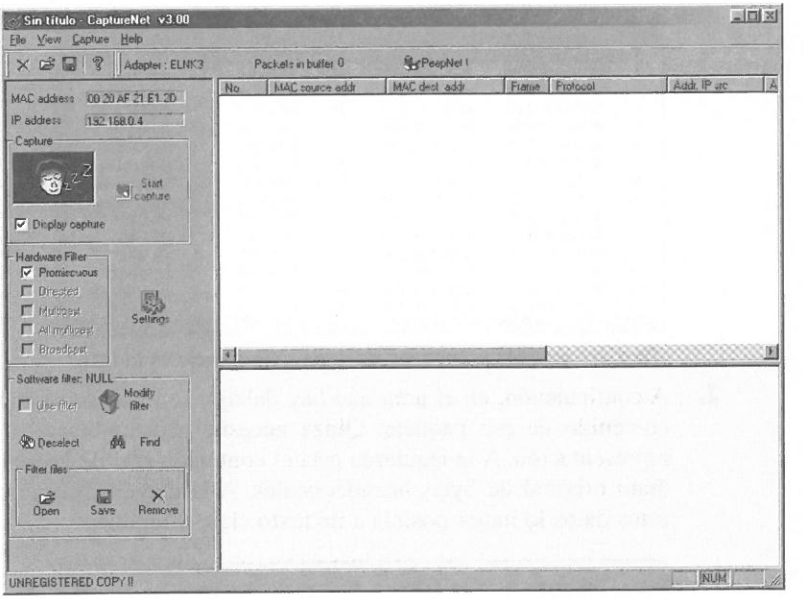
Seleccione en primer lugar el adaptador de red que debe vigilar CaptureNet.

2. Para que CaptureNet pueda configurar adecuadamente el controlador de la tarjeta de red, tras haber elegido un adaptador deberá volver a arrancar el programa otra vez. Una ventana de advertencia especial se lo pedirá. Sólo si ha tenido lugar el reinicio, CaptureNet podrá iniciar con éxito su actividad de fisgoneo.



Tras la elección del adaptador de red que debe ser vigilado, hay que reiniciar CaptureNet.

3. A continuación, el programa mostrará su interfaz habitual. La zona situada en el margen izquierdo de la ventana contiene todos los elementos de control más importantes. A la derecha aparecerán posteriormente los paquetes de datos espiados y su contenido.



La interfaz de CaptureNet.

4. Para poder iniciar el análisis del tráfico de datos, haga clic en el botón *Start capture*, situado en la parte superior de la barra de control. CaptureNet empezará a registrar todos los paquetes de datos que pasen a través del adaptador de red elegido. En la lista situada en la parte superior derecha se mostrará una relación cronológica de los paquetes. Para cada paquete, recibirá los datos esenciales, como la dirección del remitente y la del destinatario, o el protocolo empleado. En función de la intensidad del tráfico en la red, la lista podrá llenarse muy deprisa.

5. Durante el proceso de fisgoneo, el botón de *Start capture* se ha convertido en un botón de *Stop Capture*. Haga clic sobre el mismo cuando quiera parar el proceso de fisgoneo.

Analizar los datos

Cuando el sniffer se haya ejecutado durante un rato, seguramente habrá recopilado una buena cantidad de paquetes de datos. CaptureNet ofrece una posibilidad sencilla para ver el contenido de estos paquetes de datos. Si contienen textos claros, como contraseñas, mensajes de correo electrónico o archivos de texto, se puede leer directamente su contenido.

1. Para analizar los datos recopilados, haga clic en uno de los paquetes de datos registrados. Lo mejor es que empiece por los de arriba del todo.

No	MAC source addr	MAC dest addr	Frame	Protocol	Addr IP src
3	00 20 AF 0B 6A FA	FF FF FF FF FF FF	802.3	IPX	No IP Address
4	00 20 AF 59 50 94	00 20 AF 21 DE DC	802.3	IBM Netbios	No IP Address
5	00 20 AF 21 DE DC	00 20 AF 59 50 94	802.3	IBM Netbios	No IP Address
6	00 4F 49 0B 67 FD	00 20 AF 59 50 94	IP	TCP->HTTP	204.198.135.85
7	00 20 AF 59 50 94	00 4F 49 0B 67 FD	IP	TCP->HTTP	192.168.0.6
8	00 20 AF 49 CA C5	00 20 AF 21 DE DC	802.3	IBM Netbios	No IP Address
9	00 20 AF 21 DE DC	00 20 AF 49 CA C5	802.3	IBM Netbios	No IP Address
10	00 20 AF 59 36 1A	00 4F 49 0B 67 FD	802.3	IBM Netbios	No IP Address
11	00 4F 49 0B 67 FD	00 20 AF 59 36 1A	802.3	IBM Netbios	No IP Address
12	00 20 AF 59 50 94	00 4F 49 0B 67 FD	IP	TCP->HTTP	192.168.0.6
13	00 20 AF 59 50 94	00 4F 49 0B 67 FD	IP	UDP->DNS	192.168.0.6
14	00 4F 49 0B 67 FD	00 20 AF 59 50 94	IP	UDP->DNS	192.168.0.1
15	00 20 AF 59 50 94	00 4F 49 0B 67 FD	IP	TCP->HTTP	192.168.0.6
16	00 4F 49 0B 67 FD	00 20 AF 59 50 94	IP	TCP->HTTP	216.77.103.179
17	00 20 AF 59 50 94	00 4F 49 0B 67 FD	IP	TCP->HTTP	192.168.0.6

Para ver uno de los paquetes de datos, selecciónelo en la lista.

2. A continuación, en el área que hay debajo, se mostrará detalladamente el contenido de ese paquete. Quizá necesite acostumbrarse al formato de representación. A la izquierda está el contenido real de los datos en el formato original de bytes hexadecimales. A la derecha, CaptureNet traduce estos datos lo mejor posible a un texto claro y legible.

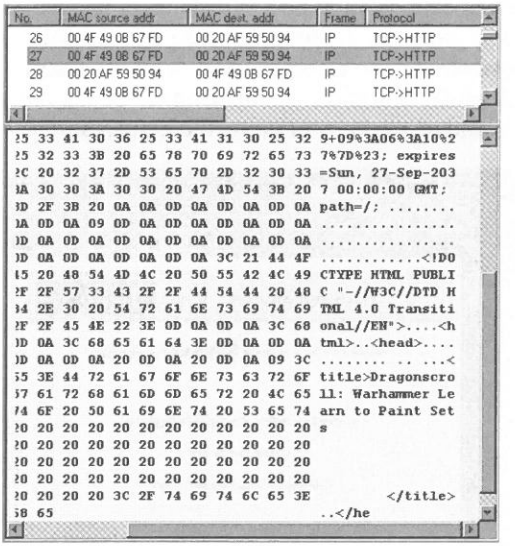
```
0000:  FF FF FF FF FF FF 00 20 AF 0B 6A FA 00 25 E0 E0  ....... ..j..%..
0010:  03 FF FF 00 22 00 11 00 00 00 00 FF FF FF FF FF  ....".....
0020:  FF 04 52 00 00 00 00 00 20 AF 0B 6A FA 40 08 00  ..R..... ..j.@.
0030:  03 00 04 04 04 04 04 04 04 04 04 04              ..........
```

El contenido de los paquetes de datos aparece en un formato al que usted quizá necesite acostumbrarse.

3. Lo más práctico sería que utilice las teclas de las flechas para recorrer por orden los paquetes de datos visualizados en la parte superior. Así, en la de abajo verá siempre el contenido del paquete recién seleccionado. Si parece

interesante, podrá cambiar al área de contenido para estudiarlo más de cerca.

Según el tipo de tráfico de datos, usted encontrará muchos paquetes de datos en los que no se pueda apreciar ningún contenido reconocible. Una parte nada desdeñable del tráfico en la red consiste en lo que se denomina como "overhead". Se trata de noticias de administración que sirven para la sincronización y autoorganización del tráfico en la red. Pero siempre que haya un intercambio de datos en texto claro, estos podrán ser trasladados a formato visible. Por ejemplo, esto se da en las transmisiones donde se envían textos sencillos sin encriptar, como puede ser al leer y escribir mensajes de correo electrónico o al intercambiar documentos de texto. Incluso las contraseñas (por ejemplo, de una dirección de correo electrónico) pueden ser leídas en el momento de iniciarse la sesión si el procedimiento de introducción no las transmite encriptadas por la red.



El texto que sea transmitido sin encriptar puede ser leído sin problemas por un sniffer de paquetes.

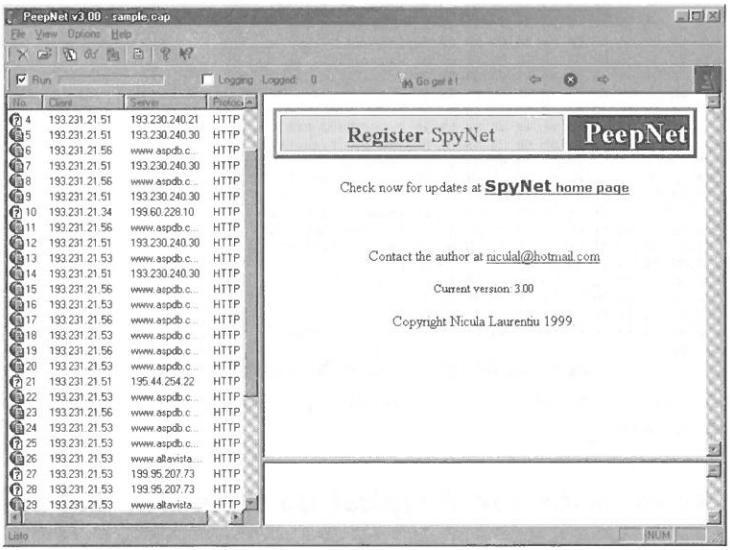
Preparación con PeepNet de los datos del sniffer

Como habrá podido apreciar en los experimentos realizados con CaptureNet, dentro del sniffer sólo se pueden ver los contenidos de texto, y eso con bastante esfuerzo. Pero SpyNet también incluye PeepNet, que permite un análisis más cómodo de los datos recopilados. PeepNet es capaz de analizar todos los datos reunidos y de relacionarlos entre sí. De este modo, los paquetes de datos vinculados permiten reconstruir fácilmente los procesos de comunicación al comple-

to. Esta herramienta hace posible, por ejemplo, reproducir la bajada del correo electrónico a través de POP incluyendo la contraseña de POP y todos los contenidos de los mensajes, si antes de eso se captaron todos los paquetes de datos correspondientes. Lo mismo se puede aplicar a las sesiones de navegación por la Red, donde se pueden reconstruir las páginas web visitadas por un internauta desde otro PC.

1. Si arranca PeepNet directamente desde CaptureNet con un clic sobre el botón *PeepNet!*, éste se hará cargo automáticamente de los datos de la vigilancia de paquetes que esté en curso. Como alternativa, también puede guardar los datos recopilados con CaptureNet e importarlos a continuación a PeepNet (con *File/Open*).

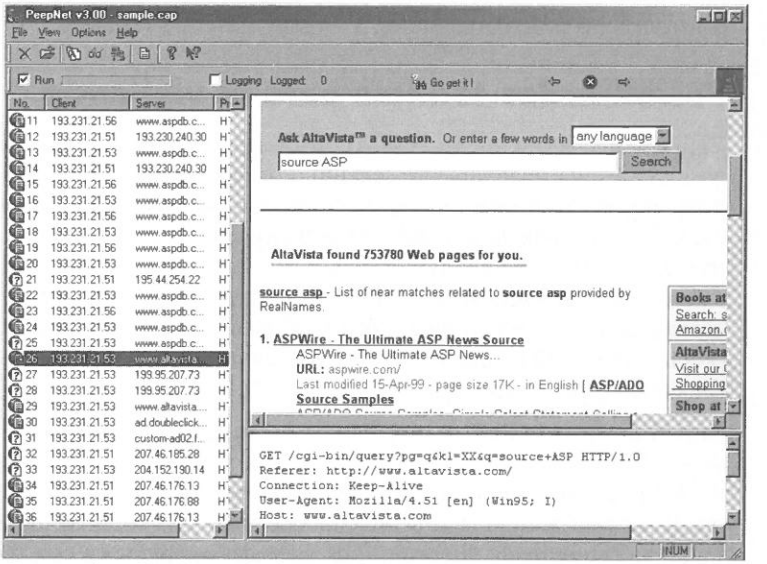
2. En ambos casos, PeepNet analiza los datos e intenta reconstruir, a partir de los paquetes de datos, vínculos de comunicación coherentes. Cada vez que lo consiga, generará una entrada en la lista situada en el margen izquierdo de la ventana. Por el símbolo que figure delante de ésta, se puede reconocer el tipo de comunicación, por ejemplo, si se trata de páginas web o correo electrónico. Además, se indican las direcciones de los ordenadores que participaran en la comunicación y el protocolo empleado.



PeepNet muestra a la izquierda los vínculos de comunicación reconstruidos.

3. Para reconstruir la respectiva comunicación, sólo hay que seleccionar la correspondiente entrada en la lista. PeepNet preparará el contenido lo mejor que pueda. Si, por ejemplo, se trata de la visita a una página web, PeepNet representará la página correspondiente. Esta información la extrae sutil-

mente de los paquetes de datos recogidos, no llamando sin más a la página web desde Internet. De este modo es posible reconstruir hasta páginas web confidenciales que sólo permitan ser llamadas con una contraseña.



En este ejemplo, el usuario de un ordenador fisgoneado había hecho una consulta a AltaVista.

4. Aparte del contenido en sí, PeepNet también visualiza en la parte de abajo todos los datos que puedan ser extraídos de los paquetes fisgoneados. En las páginas web, esto incluye el software implicado (por ejemplo, el navegador web que se utilice) y, cuando es posible, también el sistema operativo.

6.3 Vigilancia en el puesto de trabajo – ¿Qué es factible y está permitido?

Cada vez hay más empresas que aprovechan las rápidas y baratas posibilidades de comunicación de la Red. A fin de cuentas, Internet ofrece acceso a infinidad de información actualizada, que para muchos colectivos profesionales supone una gran ayuda o incluso resulta imprescindible, por lo que los jefes ponen a disposición de sus empleados accesos a Internet y direcciones de correo electrónico. Naturalmente, esto supone una fuerte tentación de aprovechar ese acceso también para fines no del todo profesionales. Un archivo de MP3 es bastante grande, pero a través del rápido acceso de la empresa es posible descargar sin problemas todo un CD durante el descanso de mediodía. A fin de cuentas, este tipo de acceso a Internet pagado por la empresa suele ser muy barato y mucho

más rápido que conectarse en casa vía módem o con una tarjeta RDSI. ¿A quién va a molestar algún que otro mensaje privado de correo?, piensan muchos. Pero, cuidado: eso puede acabar muy mal. En la mayoría de los casos, no se permite utilizar Internet para fines privados. Si el jefe se huele algo, la cosa podrá tener consecuencias jurídico-laborales. Y es muy fácil que se entere.

Posibilidades técnicas para la vigilancia

Vigilar lo que hacen los empleados con los accesos a Internet que tienen a su disposición resulta relativamente sencillo. Por regla general, las redes de empresa están conectadas a Internet con un ordenador especial llamado router. Es decir, todos los datos que entren en Internet o salgan del mismo pasan a través de ese router. Esto se presta maravillosamente a instalar un software de vigilancia que controle de modo selectivo a determinados empleados o busque a nivel general accesos concretos y notifique quién es el autor. En la mayoría de los casos, los propios routers disponen de funciones de monitorización que permiten hacer un seguimiento de los accesos.

Para el acceso a la Red, se emplea con frecuencia un servidor proxy propiedad de la empresa, que no sólo permite navegar más deprisa a menor precio, sino también controlar quién lo hace. En el correo electrónico, el software de red puede ser configurado fácilmente para que envíe una copia de todos los mensajes a una determinada dirección. Los mensajes recibidos en esta dirección pueden ser explorados, por ejemplo, mediante la búsqueda de un texto completo, para ver si contienen determinados términos. Si el jefe quiere saber lo que piensan sus empleados de él, le bastará con solicitar la exploración de los mensajes de correo electrónico en busca de su nombre.

No existe ninguna protección contra estas medidas de vigilancia. Además, ésta sólo podría consistir en que usted camufle perfectamente sus actividades privadas. Por supuesto que podría encriptar los mensajes de correo electrónico personales y escapar así a la vigilancia. Pero, por otra parte, levantaría sospechas precisamente por eso. La encriptación sólo resulta recomendable si está expresamente autorizado el uso personal de los recursos y usted sólo quiere protegerse de compañeros de trabajo o administradores de sistema indiscretos.

¿Justicia ante todo? – esto es lo que el jefe tiene derecho a saber sobre usted

Técnicamente, la vigilancia total es posible. Pero, ¿está permitida? El derecho laboral contiene algunas disposiciones sobre la vigilancia de equipos de comunicación. No fueron establecidas precisamente pensando en Internet, pero pue-

den ser aplicadas a este ámbito. Para no aburrirle ahora con formulaciones jurídicas, vamos a resumir el asunto en cristiano.

¿Está permitido emplear los equipos de comunicación de la empresa para cuestiones personales?

Eso depende enteramente del empresario. El mero hecho de disponer de un acceso a Internet, no autoriza a usarlo para asuntos personales. Más bien es el empresario quien debe definir su postura ante esta utilización personal. Aquí, pueden darse varias posibilidades:

- El uso para fines personales puede estar rigurosamente prohibido. Esta prohibición debería ser respetada, ya que generalmente las infracciones pueden ser causa de amonestación y, en caso de repetirse, constituir incluso motivo de despido. Y si ahora piensa "¡Bah, si no se va a enterar nadie!", le recomendamos que vuelva a leer concienzudamente el apartado anterior, donde hablamos de las posibilidades técnicas.
- Puede estar permitido a nivel general el uso para fines personales. ¡Qué bien, tener un jefe tan generoso! También aquí podría haber restricciones y condiciones para la utilización. Además, sería conveniente respetar algunas reglas de comportamiento que expondremos en el siguiente apartado.
- El uso de recursos para fines personales puede estar permitido, pero el empleado debe correr con los gastos. En el caso del teléfono en las oficinas, este arreglo no es ninguna rareza. Aunque allí, es fácil pulsar un determinado botón antes de iniciar la conversación privada. En el correo electrónico y el acceso a Internet, eso ya resulta más difícil. Sin embargo, también a esto se le pueden encontrar soluciones. Aunque, en acuerdos de este tipo, debería vigilar que sus facturas por uso privado no hagan pensar a su jefe que pasa medio día navegando por la red por diversión personal. En cuestiones de uso privado del teléfono, ya se han dado casos de despido por exceso de telefonitis.

De todos modos, debería informarse bien sobre las regulaciones del uso privado en su empresa y respetarlas. Aunque sean directrices cuyo cumplimiento no se controle rigurosamente, un compañero envidioso podría aprovechar las infracciones para hacerle daño.

¿Está permitido vigilar las comunicaciones de los empleados?

Aunque disponga de los medios técnicos, el jefe no tiene permiso para leer cualquier cosa. Pero en este caso rigen las siguientes excepciones:

- Si el empresario ha dado expresamente su consentimiento, la vigilancia es legal. ¿Que usted no lo ha hecho? Bueno, entonces quizá sea mejor que saque su contrato de trabajo y lea atentamente la letra pequeña. ¡Por si acaso!
- Es posible que la naturaleza de su trabajo exija vigilancia. Originalmente, esta regulación se refería a la vigilancia por cámara y autoriza la colocación de cámaras en las cajas y ventanillas de los bancos, por ejemplo. Aplicado a Internet, esto se podría referir a empleados que trabajen en áreas relevantes para la seguridad.
- Finalmente, una causa o sospecha justificada podría autorizar la vigilancia. Por ejemplo, si el jefe tiene razones para suponer que documentos importantes de la empresa están siendo enviados a la competencia por correo electrónico, puede vigilar la correspondencia electrónica para averiguar quién es el malhechor.

Si al hacer una vigilancia de este tipo se detecta un uso privado ilícito, el empresario puede pedir cuentas a su empleado. Es de suponer que un único incidente no será motivo de despido, pero podría traer consigo una amonestación o la reclamación de daños y perjuicios. De repetirse la infracción, habría que contar con el despido.

INFO

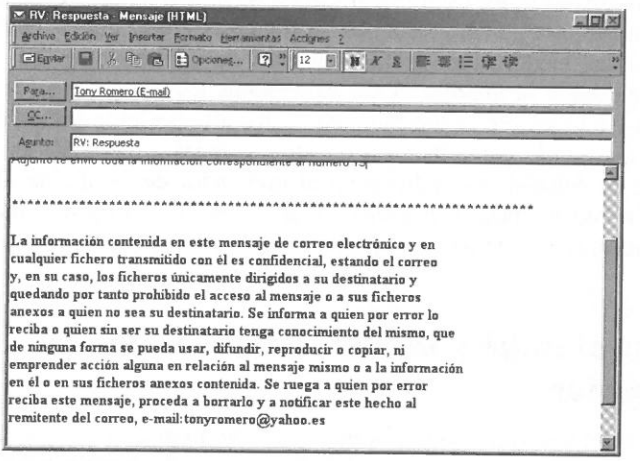
¿Tiene el jefe permiso para leer los mensajes de correo electrónico?

Por norma, no está autorizado a vigilar la correspondencia por correo electrónico de los empleados. Esto rige tanto para los superiores como también para el administrador del sistema. Y no es aplicable sólo a los mensajes privados, sino también a los de trabajo. Supondría una intromisión ilícita en la esfera privada del empleado y, por lo tanto, está prohibida. Sin embargo, se contemplan situaciones excepcionales, como puede ser cuando el empleado está de vacaciones o enfermo. En ese caso, la empresa podría tener un gran interés en que la bandeja de correo de ese empleado siga siendo vaciada. Antes de irnos de vacaciones, siempre podremos pedir a un compañero de confianza que se encargue de eso. Pero en caso de accidente o enfermedad repentina, no dispondremos de esa posibilidad. Por eso, lo mejor sería separar tajantemente los mensajes privados de los laborales. O, al menos, no recibir en la empresa mensajes privados que sean verdaderamente confidenciales. En caso de permitirse mensajes privados, una buena alternativa sería emplear un software de encriptación (por ejemplo, PGP). También resulta recomendable, porque los jefes y, sobre todo, los administradores del sistema no siempre respetan la prohibición de no leer el correo.

Las reglas de oro – así debe actuar

Tanto si se permite el uso privado como si no, hay algunas reglas que debería tener en cuenta para evitarse problemas y disgustos. Y no nos referimos sólo a los aspectos legales, sino también al ambiente en el trabajo.

- Cuando navegue por Internet, a ser posible, abra sólo las páginas serias. Siempre se puede colar el banner de un sitio de sexo, pero si usted solicita directamente *www.playboy.com*, no quedará lugar a dudas. Eso no está bien visto, aunque sólo sea porque las compañeras podrían sentirse insultadas. En algunos países, sólo con eso bastaría para poner una querella contra su empresa por acoso sexual en el trabajo.
- Lo que jamás diría en una circular, tampoco debería ponerlo en un correo electrónico. En la empresa, las broncas entre compañeros y los chistecitos sobre el jefe podrían caer fácilmente en malas manos.
- Si usted emplea para fines personales la dirección de correo electrónico de la empresa, debería dejar claro que los mensajes son privados. Sobre todo si envía alguno a grupos de noticias, listas de mailing o similares foros de discusión públicos, le recomendamos introducir en la firma un texto de advertencia. Este debería advertir expresamente de que ese mensaje es sólo su opinión personal y no refleja ningún criterio oficial de su empresa.



Un ejemplo de texto de advertencia.

- Aunque se permita el uso personal, no exagere. Si usted siempre está entre los primeros a la hora de transferir datos, o cada día recibe tanto correo electrónico que sólo para leerlo se le va por lo menos una hora de trabajo, no dude que su jefe inspeccionará el asunto durante algún tiempo.

- Piense siempre que hay todo tipo de posibilidades para la vigilancia, aunque quizá legalmente no estén permitidas. En ese caso, su jefe no podría echarle en cara sus infracciones, pero estaría al corriente de ellas. En la siguiente ronda de ascensos, a la hora de negociaciones salariales o si hay que reducir la plantilla, esta información quizá podría tener una influencia decisiva.

TRUCO

Directrices concretas para el uso de Internet

Siempre que en una empresa se pueda usar Internet, deberían existir directrices claras y concisas sobre qué está permitido a los empleados y qué no. En las empresas grandes, generalmente, ya las suele haber. Y si no, el comité de empresa debería ocuparse de que sean redactadas y publicadas. Pero también en las empresas pequeñas resultan muy convenientes para proteger a los empleados de que sus superiores les den permisos verbales precipitados y, de pronto, se retracten.

6.4 Borrar las huellas delatoras de su navegación por Internet

En el PC de la oficina hay que tener siempre mucho cuidado con los datos privados. Si el empresario ha prohibido rotundamente que se usen el PC e Internet para fines privados, los asuntos personales no pintan nada en el ordenador. Pero si alguna que otra vez nos saltamos las directrices, deberíamos cuidarnos de no dejar huellas inequívocas. Incluso en caso de permitirse un uso privado, no habría que bajar la guardia. A fin de cuentas, los compañeros de trabajo son curiosos y no siempre se detienen ante datos a todas luces personales. Por eso, todo lo que jamás contaríamos a nuestros colegas a mediodía en el comedor, tampoco lo deberíamos archivar en el ordenador de la oficina al alcance de todos. En este apartado queremos exponer los diferentes tipos de datos y darle a usted consejos para emplear sin problemas sus datos personales en el PC del trabajo.

Borrar el caché y los datos de historial del navegador

Los navegadores web modernos dan gran importancia a la manejabilidad y la comodidad. Disponen de diversas funciones, cuya finalidad es hacer la vida más fácil al usuario. Pero tanta comodidad también tiene sus desventajas. Los navegadores registran información sobre los intereses y las costumbres de los usuarios. En principio, cualquiera que tenga acceso al ordenador puede ver esos datos. ¿Quizá usted tenga en su trabajo un acceso a Internet que de vez en cuando usa para su esparcimiento personal? ¿O quizá visite alguna vez páginas web

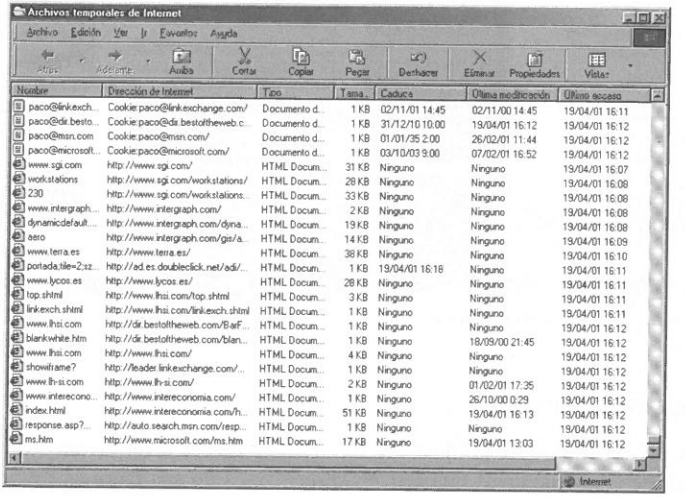
de las que no deban enterarse sus compañeros de trabajo o (si se trata de su PC particular) sus hijos? Los datos antiguos almacenados permiten a cualquiera, con un simple clic del mouse, averiguar las páginas web que usted visitó en los últimos tiempos.

¿Qué datos están en peligro?

Los navegadores web almacenan diversos tipos de datos sobre las actividades de sus usuarios, para que en caso de necesidad puedan ser llamados con más rapidez y comodidad. Pero eso no sólo lo puede hacer el usuario legítimo, sino en principio cualquiera que acceda a ese ordenador después de él.

Un protocolo de navegación detallado en el caché de Internet

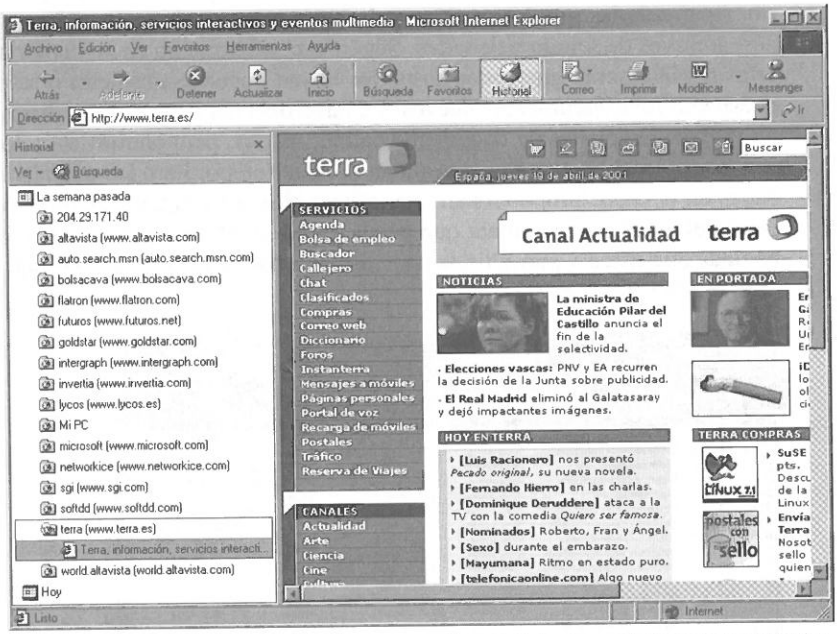
En el caché de Internet se guardan todos los documentos solicitados por el usuario. Aparte de las propias páginas web, entre estos también se incluyen imágenes, archivos de sonido y de vídeo. Según la configuración de la memoria caché, estas páginas serán guardadas hasta que hayan quedado obsoletas o se necesite el espacio para documentos nuevos. La tarea del caché es resolver directamente las nuevas peticiones de documentos almacenados, para ahorrar así a los usuarios conexiones on-line que consuman mucho tiempo. Pero las páginas almacenadas en el caché proporcionan una información muy detalladas sobre los intereses del usuario. Cualquiera que pueda entrar en el ordenador, podrá saber las páginas que usted visitó últimamente, incluyendo la hora exacta en que se produjo el acceso.



En el caché de Internet se registran todos los documentos web de las últimas sesiones de navegación, incluyendo la hora exacta en que tuvo lugar el acceso.

El historial

El historial de los navegadores almacena las direcciones visitadas. Esto tiene como finalidad que, cuando el usuario vuelva a visitar una página, simplemente pueda seleccionar la dirección en la lista del historial sin necesidad de teclear otra vez el URL completo. Además, esta función se emplea para completar el URL, lo cual resulta muy práctico. Si una dirección URL es ya conocida, basta con teclear los primeros caracteres en el campo de dirección del navegador. En cuanto este sepa inequívocamente de qué dirección se trata, la completará de modo automático. También en este caso, la comodidad del usuario puede volverse contra él. Igual que el caché, el historial de navegación informa con detalle sobre las actividades del usuario. Si otra persona tiene acceso a su PC, podrá averiguar inmediatamente a qué direcciones se conectó en los últimos días o semanas.



Desde el Historial de Internet Explorer se pueden abrir incluso páginas web visitadas hace semanas.

Marcapáginas chivatos

Finalmente, otra fuente de peligro son los marcapáginas o favoritos. Todo navegador permite a sus usuarios guardar las direcciones de sus páginas favoritas, de modo que pueda acceder a ellas cómoda y rápidamente. Pero también estos datos

proporcionan a personas no autorizadas información sobre los intereses y las preferencias del usuario. A fin de cuentas, nada impide a un intruso cotilla abrir los favoritos que usted tenga guardados. En realidad, aquí está la fuente de peligro más importante. Mientras el acceso al caché y al historial requiere al menos ciertos conocimientos básicos, no hace falta saber gran cosa para llamar a los favoritos, que en la mayoría de los navegadores van integrados directamente en la barra de menús. Pero, en cambio, la medida de protección a aplicar es muy sencilla. Desista sin más de guardar las direcciones web como marcapáginas si no quiere que otros las sepan.

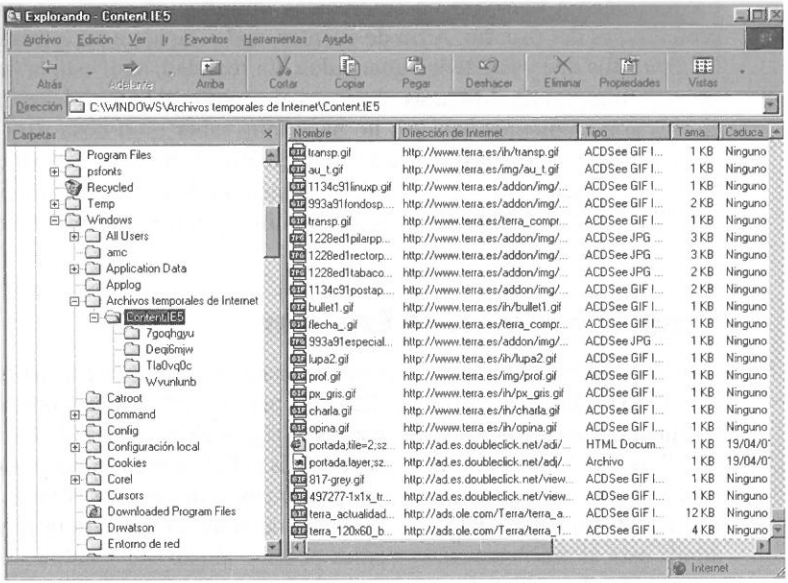
El caché de Internet Explorer

También Internet Explorer dispone de una zona de memoria intermedia donde guarda todas las páginas web solicitadas por el usuario. Estas permanecerán allí aunque el usuario ya haya cambiado a la siguiente página. Sólo cuando el caché esté lleno, se borrarán los documentos más antiguos para hacerles sitio a los nuevos. Si llama una página que visitó hace poco, el navegador la sacará mucho más deprisa directamente del caché que obteniéndola otra vez de Internet. Y aquí es donde está el problema. Esta técnica permite almacenar localmente (en función del tamaño del caché) las páginas web de las páginas visitadas durante los últimos días o las últimas semanas. De modo que el jefe o un "compañero" podrían averiguar con toda facilidad en el caché si realmente usó el acceso a Internet de la empresa para fines profesionales, o incluso informarse sobre las páginas web que visitó durante los últimos días.

Todo lo que almacena el caché

¿Quiere comprobar por sí mismo todo lo que tiene almacenado ahora en el caché de Internet de su PC? Entonces, haga lo siguiente:

1. Con *Herramientas/Opciones de Internet*, abra el cuadro de diálogo de configuración de Internet Explorer.
2. En la categoría *General*, haga clic sobre el botón *Configuración* del apartado *Archivos temporales de Internet*.
3. Aparecerá el cuadro de diálogo *Configuración*, donde deberá hacer clic en *Ver archivos*. Esto abrirá una ventana del Explorador de Windows, mostrando la carpeta donde se almacenan los archivos temporales de Internet.



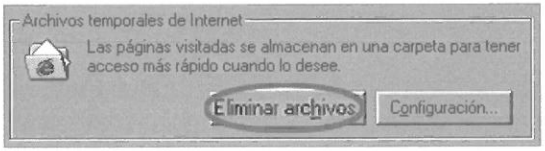
El caché de Internet: el espacio de almacenamiento de Internet Explorer.

4. Aparte del nombre, tamaño y fecha, en la lista también podrá ver el servidor web desde el cual fueron descargados los respectivos objetos. ¿Le sorprende la buena "memoria" de Internet Explorer?

Vacíe el caché de Internet Explorer

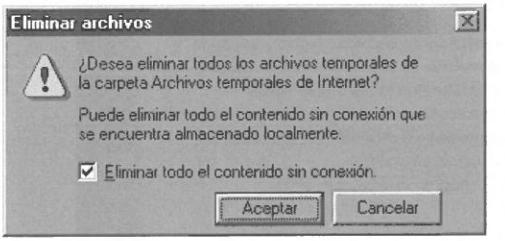
Si quiere evitar que el caché de Internet Explorer delate sus hábitos de navegación a otras personas, debería borrarlo con regularidad. Como alternativa, también podría vaciarlo cada vez que haya visitado páginas que de alguna forma puedan ser comprometedoras.

1. Para vaciar el caché, abra el cuadro de diálogo de configuración con *Herramientas/Opciones.*
2. En el apartado *Archivos temporales de Internet*, haga clic en el botón *Eliminar archivos* para deshacerse de las páginas almacenadas en el caché.



Así borrará el caché de Internet en Internet Explorer.

3. Antes de limpiar el caché, Internet Explorer le pedirá una confirmación por si acaso. Conteste a la consulta de seguridad pulsando sobre *Aceptar*. Si también quiere eliminar las referencias off-line de los contenidos sin conexión almacenados localmente, active antes la opción *Eliminar todo el contenido sin conexión*.



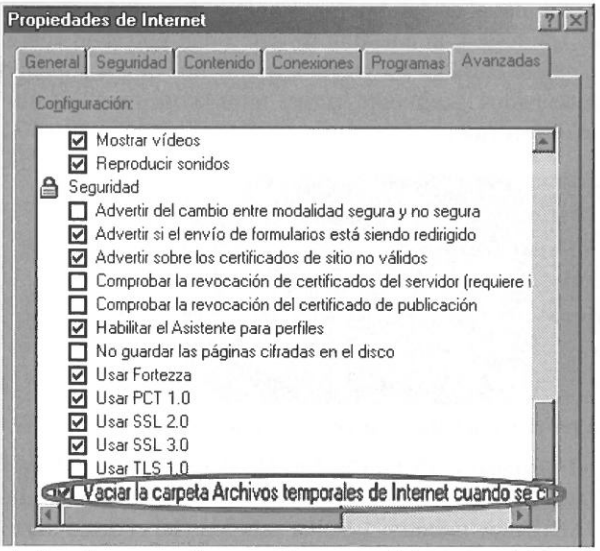
Para borrar, confirme con Aceptar la consulta de seguridad.

4. Ahora, el navegador vaciará la carpeta del caché. Según su tamaño, esto podrá llevar algunos minutos por lo que, en caso de duda, debería conceder a su PC un tiempo mientras perciba actividad en el disco duro. Después, su PC estará libre de huellas delatoras de navegación.

Configurar el borrado automático del caché

También puede automatizar el borrado del caché si lo que desea es que quede limpio después de cada sesión. Internet Explorer dispone de una opción extra en su configuración avanzada de seguridad.

1. Acceda a *Herramientas/Opciones de Internet* y pulse sobre la pestaña *Avanzadas*.
2. Busque en la lista de configuraciones el apartado *Seguridad*.
3. Aquí encontrará la opción *Vaciar la carpeta Archivos temporales cuando se cierre el explorador*, que se encargará de borrar automáticamente el caché cuando cierre Internet Explorer.



Activando esta opción, se realiza automáticamente el borrado del caché de Internet Explorer al finalizar la sesión.

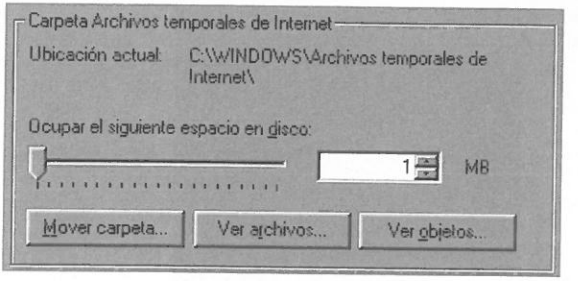
4. Confirme la nueva configuración con *Aceptar*.

Desde este momento, cada vez que se cierre Internet Explorer, se borrarán automáticamente los datos almacenados en el caché. De este modo, al menos se dispone del efecto acelerador del caché durante una sesión de navegación. Pero si se bloquea Internet Explorer (¡según dicen, ocurre alguna que otra vez!), este ya no podrá borrar el caché, con lo que sus datos permanecerán almacenados hasta la próxima vez que se cierre correctamente el navegador, o hasta que sean borrados manualmente.

Desactivar el caché de Internet Explorer

Si usted no quiere repetir el borrado del caché de Internet tras cada sesión de navegación, también puede desactivarlo. Así no corre ningún riesgo, pero renuncia al efecto acelerador del caché.

1. Dentro de las opciones generales de Internet, haga clic en el botón *Configuración* para mostrar las opciones del caché de Internet.
2. En *Ocupar el siguiente espacio en disco* podrá reducir el espacio hasta el mínimo posible. El valor mínimo permitido es 1 Mb, con lo cual el caché quedaría casi totalmente anulado.
3. Guarde las nuevas configuraciones haciendo clic dos veces *sobre Aceptar*.



Ajustando el tamaño, el caché de Internet Explorer prácticamente puede ser desactivado.

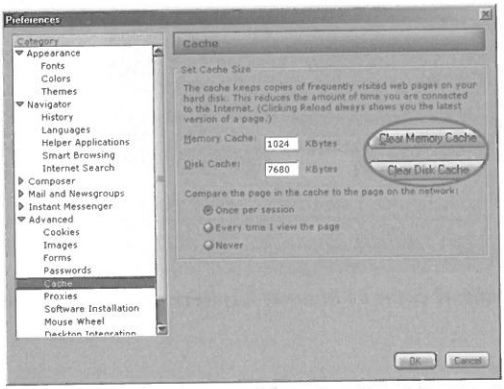
El caché de Netscape Navigator

Igual que Internet Explorer, también Netscape Navigator dispone de un caché para páginas web donde, durante cierto tiempo, se almacenan localmente las páginas web que fueran transmitidas alguna vez, para poder responder con más rapidez cuando sean llamadas de nuevo. El caché de Netscape Navigator es algo más discreto, ya que sustituye los nombres y las imágenes de las páginas web por expresiones criptográficas que sólo entiende el propio navegador. Por lo tanto, no bastará con echar un vistazo a la carpeta del caché para averiguar las últimas páginas que usted visitó. Sin embargo, también proporciona la posibilidad de abrir y examinar los archivos y las imágenes HTML renombradas de modo que, al final, es posible obtener información sobre su contenido.

Borre el caché de Netscape Navigator

El caché de Netscape Navigator puede ser borrado en cualquier momento para eliminar del disco duro las páginas web potencialmente comprometedoras. Así no podrán ser descubiertas por otros, ya sea intencionadamente o por casualidad.

1. Abra las configuraciones de Netscape Navigator con *Edit/Preferences* y acceda a la categoría *Advanced/Cache.*
2. Con los botones *Clear Memory Cache* y *Clear Disk Cache* eliminará los datos del caché de la memoria o del disco duro (por razones de eficacia, Netscape Navigator posee un sistema de caché de dos niveles).



Netscape Navigator permite vaciar el caché en cualquier momento.

Desactivar el caché de Netscape Navigator

Si para mayor seguridad desea renunciar totalmente al caché de Netscape Navigator, también lo podrá hacer. En la pantalla de configuración del caché (ver más arriba), puede delimitar el espacio de memoria disponible para los datos de caché. Si quiere desactivarlo por completo, le ayudará el siguiente truco: ponga todos los valores a 0. Por cierto, el caché de memoria lo puede dejar tranquilamente activado. Los datos almacenados en él desaparecen cuando cierre el navegador.

Los datos del Historial en Internet Explorer

Además del caché, Internet Explorer dispone de una función de historial. Al contrario de lo que ocurre en el caché, donde los datos se amontonan con bastante desorden, el historial facilita un acceso estructurado. Clasifica cronológicamente los datos almacenados en el caché por días y semanas transcurridos. Así, se pueden consultar cómodamente las páginas web del caché. En combinación con el modo off-line, permite ver con toda tranquilidad las páginas almacenadas localmente sin necesidad de establecer una conexión on-line. Desgraciadamente, para los curiosos es igual de fácil recurrir al Historial de su Internet Explorer para comprobar las páginas web que visitó y cuándo lo hizo.

INFO

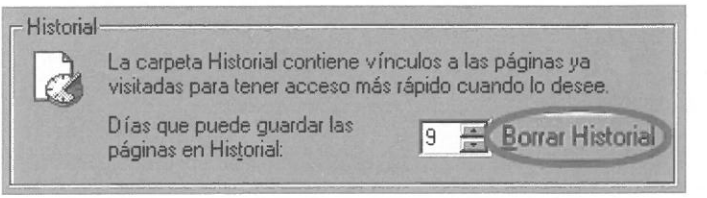
La relación entre caché e Historial

En Internet Explorer, caché e Historial no son funciones rivales. Trabajan en estrecha relación. El caché almacena las páginas web descargadas, mientras que el historial sólo registra el nombre de las páginas y el momento en que fueron solicitadas. Si desde la barra de Historial se llama a una determinada página web de una sesión anterior, el historial la extrae del caché. Esta colaboración permite deducir que no basta con borrar sólo el caché o sólo el Historial, ya que los datos del otro serían conservados. Para ir a lo seguro, deberá poner orden tanto en el caché como en el Historial.

Borre los datos en el Historial de Internet Explorer

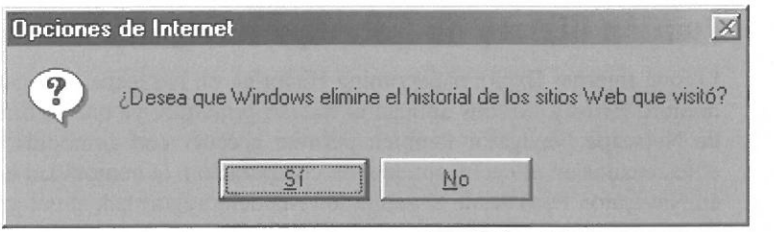
Para que el Historial no revele información confidencial, puede borrar cuando quiera los datos almacenados en él:

1. Abra *Herramientas/Opciones de Internet*. En el apartado *Historial*, situado en el extremo inferior de la ventana, encontrará la configuración del Historial.
2. Con el botón *Borrar Historial* eliminará todas las direcciones que tenga almacenadas en ese momento el Historial.



Así puede borrar las direcciones almacenadas en el Historial.

3. Aunque antes, Internet Explorer le volverá a preguntar para evitar un borrado accidental. Confirme la consulta de seguridad con *Sí*.



Confirme la consulta de seguridad para vaciar el Historial.

TRUCO

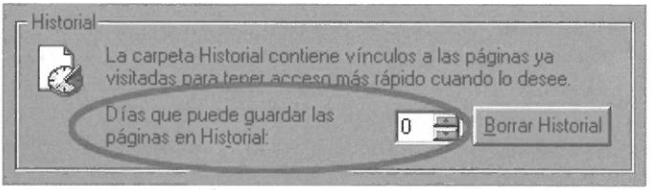
Borrar entradas concretas del Historial

Como en realidad el Historial es una función bastante práctica, sería una pena tener que borrar por culpa de un pequeño desliz todos los datos almacenados trabajosamente durante las sesiones de navegación. Pero, por suerte, también disponemos de una función para borrar selectivamente entradas concretas del Historial. Abra el Historial y haga clic con el botón derecho del mouse en la entrada correspondiente. En el menú contextual que aparecerá verá el comando *Eliminar*, que le permitirá borrar la entrada del Historial tras haber confirmado la consulta de seguridad. Pero este borrado sólo afectará al Historial; la página en cuestión seguirá almacenada en el caché.

Desactivar completamente el Historial

Como el Historial consume lo suyo en espacio en disco, Internet Explorer permite indicar los días que deberán ser almacenados los datos históricos. Se puede poner fuera de combate al Historial empleando un pequeño truco. Si reduce el número de días a 0, el Historial prácticamente dejará de registrar los datos.

1. Abra *Herramientas/Opciones de Internet*.
2. Introduzca un *0* en el campo *Días que puede guardar las páginas en Historial*, para que el Historial deje de almacenar la información.



Acortando el tiempo de conservación, puede dejar prácticamente fuera de combate al Historial.

3. Guarde la nueva configuración con *Aceptar*.

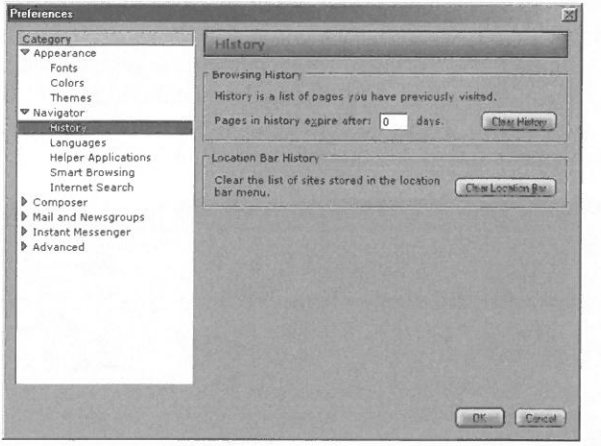
Función History en Netscape Navigator

Lo que Internet Explorer denomina Historial, en Netscape Navigator recibe el nombre History. Ambos aplican el mismo principio, ya que la función History de Netscape Navigator también permite acceder con comodidad a los datos almacenados en el caché aunque, en comparación, la comodidad es algo menor en Navigator. Pero desde el punto de vista de la seguridad, el peligro que emana de esta función es el mismo.

Borrar los datos de History

También Netscape Navigator permite desprenderse de los molestos recuerdos de pasadas sesiones de Internet:

1. Abra el cuadro de diálogo de configuración de Netscape Navigator mediante *Edit/Preferences* y acceda a la categoría *Navigator/History*.
2. Con el botón *Clear History*, situado en el apartado *Browsing History*, podrá librarse de los datos almacenados.



La configuración de History para la función de historial en Netscape Navigator.

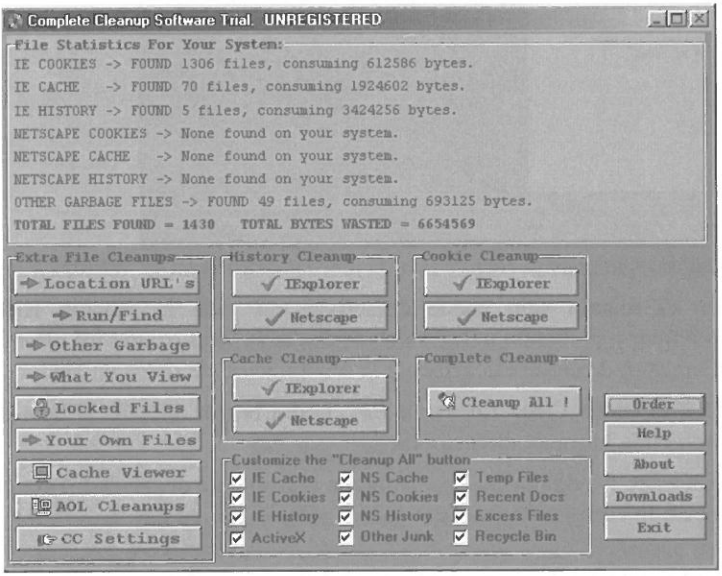
3. En el mismo sitio puede desactivar del todo la función History de Navigator, poniendo a 0 el valor de *Pages in history expire after X days*. Con esto, detendrá eficazmente la recopilación de datos en History.
4. Con el botón *Clear Location Bar*, podrá borrar además la lista de sitios web en la barra de direcciones.
5. Netscape Navigator no hace ninguna consulta de seguridad. Para concluir, cierre la ventana Preferences con un simple clic en *OK*.

Proteja cómodamente su vida privado

Por desgracia, configurar y borrar el caché del navegador lleva tiempo y es engorroso. Además, existe un considerable peligro de que en el momento decisivo, se nos olvide borrar los datos. Con lo práctico que sería disponer de un gran botón rojo que sólo hubiera que pulsar después de navegar... De hecho, esta herramienta existe y la tenemos en *Complete Cleanup*, que puede encontrar en Internet en http://members.aol.com/softdd/. Complete Cleanup es un sencillo programa shareware para Windows. Cuando lo necesite, bastará con abrirlo a través del menú Inicio. Complete Cleanup analiza en primer lugar su sistema y busca archivos e información que puedan ser borrados. Estos pueden ser:

- datos de History de Netscape Navigator,
- datos del Historial de Internet Explorer,
- datos del caché de ambos navegadores,
- cookies de ambos navegadores, así como
- otros datos que ocupen innecesariamente espacio en disco (por ejemplo, archivos temporales).

Complete Cleanup le permite borrar estos datos clasificados por categorías. Aunque aún resulta más sencillo usando el botón *Cleanup ALL!*. Este botón elimina de su sistema todos los datos potencialmente comprometedores que haya encontrado, con lo que podrá estar tranquilo cuando apague el ordenador. El manejo es muy sencillo. Todas las funciones son directamente accesibles desde la ventana principal a través de botones claramente señalados.



Con Complete Cleanup, hace sitio y pone orden en su ordenador.

Proteger las contraseñas privadas en el puesto de trabajo

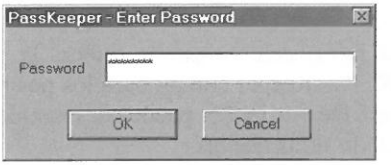
En el puesto de trabajo, usted no es el único que tiene acceso a su ordenador. También sus compañeros. Si se ausenta por vacaciones o enfermedad, nunca podrá estar seguro de que uno de sus compañeros no "tome prestado" su ordenador, ya sea con buena o mala intención. Esto repercute de un modo especial en las contraseñas. Jamás deberían ser guardadas en el PC, aunque los cuadros de diálogo correspondientes ofrezcan una opción para hacerlo. Esto permitiría a sus compañeros acceder con un simple clic del mouse a aquellos datos y funciones, que usted en realidad quería proteger.

Si usted no tiene buena memoria y teme olvidar las contraseñas importantes, no le quedará más remedio que guardarlas, sobre todo si protege otros accesos correctamente con otras contraseñas. En estos casos, hay programas para admi-

nistrar contraseñas que ofrecen un buen término medio entre comodidad y seguridad. Estos programas auxiliares guardan para todos sus accesos el nombre de usuario, la contraseña y otras informaciones que pudieran ser necesarias. Estos datos se almacenan encriptados en el disco duro y sólo se podrá acceder a ellos con una contraseña maestra, la única que tendrá que memorizar. Un programa de este tipo es PassKeeper, que podrá descargar desde http://www.passkeeper.com y utilizar gratuitamente como freeware.

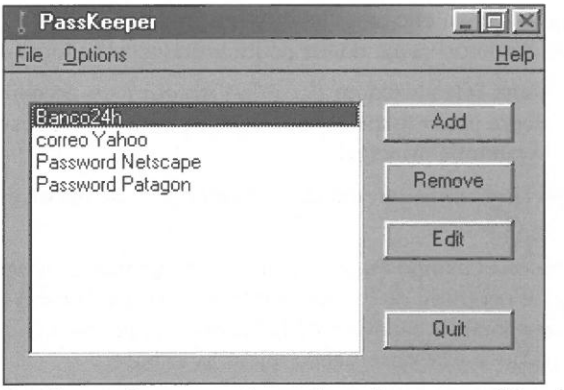
Utilice PassKeeper para proteger sus contraseñas

1. Para arrancar PassKeeper, ejecute el archivo de programa *Pass32.exe*.
2. A continuación, introduzca en la ventana de diálogo *PassKeeper – Enter Password* la contraseña maestra que ponga a su alcance todos los datos de acceso guardados.



Con PassKeeper, sólo necesita memorizar la contraseña maestra de acceso.

3. Si la contraseña es correcta, Pass Keeper mostrará su interfaz de programa. En ella encontrará una lista de los datos de acceso almacenados y podrá entrar en las funciones principales.



PassKeeper almacena todos sus datos de acceso confidenciales.

4. Si quiere ver los datos de un acceso, haga doble clic en la correspondiente entrada de la lista. PassKeeper abrirá la ventana *Edit*, donde aparecerán los datos.

Para cada entrada, aparte del nombre de usuario y la contraseña, se pueden guardar más datos.

5. Cuando haya obtenido la información deseada, cierre la ventana con *Cancel*. Al cerrarla con *OK*, PassKeeper comprobará los posibles cambios en los datos y los almacenará. De este modo, puede por ejemplo corregir las contraseñas guardadas o añadir otras nuevas.

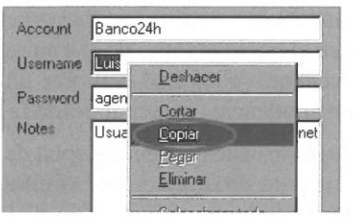
Generar las entradas de PassKeeper

1. Para almacenar en PassKeeper nuevos datos de acceso, arranque el programa e introduzca su contraseña maestra.
2. A continuación, haga clic en el botón *Add*. PassKeeper abrirá una ventana de inserción de datos vacía, donde podrá introducir los datos del acceso.
3. En primer lugar, introduzca en el campo *Account* un nombre descriptivo del acceso. Podrá poner lo que desee. La entrada aparecerá después con este nombre en la pantalla principal.
4. En el campo *Username* introduzca el nombre de usuario con el que se vaya a registrar en el acceso.
5. Teclee ahora en el campo *Password* la contraseña para el acceso. Tenga en cuenta que (al contrario de lo que sucede en otras ocasiones) la contraseña aparecerá en pantalla cuando usted la introduzca, por lo que, a ser posible, vigile que nadie le esté observando mientras lo hace.
6. En el campo *Notes* podrá introducir las observaciones y notas que desee para su propia organización.
7. Con *OK* guardará la nueva entrada.

Trasladar las contraseñas directamente a los campos de entrada de datos

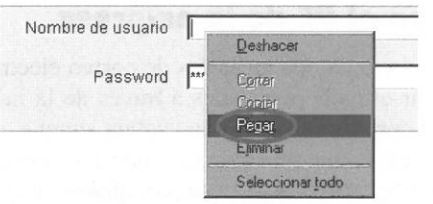
Si usted quiere abrir un acceso con contraseña, tiene que arrancar primero el software de acceso y después PassKeeper para releer los datos. Como resulta algo engorroso leer los datos en un programa y teclearlos en otro y, sobre todo, porque puede dar lugar a errores, queremos revelarle otro método que le facilitará el trabajo. Aproveche sencillamente el portapapeles de Windows para sus propios fines.

1. Arranque PassKeeper, introduzca la contraseña maestra y abra la entrada que contenga los datos requeridos.
2. Marque con el mouse el contenido del campo *Username*.
3. Ahora, haga clic en ese campo con el botón derecho del mouse y seleccione en el menú contextual la opción *Copiar*. Avanzará más deprisa si emplea las teclas *[Ctrl] + [C]*.



En lugar de perder el tiempo tecleando, puede tomar los datos de PassKeeper...

4. Cambie ahora al software de acceso y coloque el puntero del mouse en el campo de introducción del nombre de usuario.
5. Abra de nuevo el menú contextual haciendo clic con el botón derecho del mouse y seleccione la opción *Pegar*. La combinación de teclas para hacer esto es *[Ctrl] + [V]*. De este modo, copiará la entrada desde PassKeeper al software de acceso.



...e introducirlos en el campo de entrada a través del portapapeles de Windows.

6. Repita los dos pasos anteriores para la contraseña.
7. Como los últimos datos que transfirió seguirán almacenados en el portapapeles de Windows, debería realizar después otro proceso de copiado con cualquier texto inofensivo para reemplazar el contenido confidencial del portapapeles.

Este método funciona con todos los programas y campos de introducción de datos que soporten el portapapeles de Windows y se atengan a las normas pertinentes. Según ha demostrado la experiencia, puede haber problemas con los applets de Java que se ejecuten en el navegador web, como por ejemplo las interfaces de usuario de la banca por Internet. Estas no son capaces de tomar los datos desde el portapapeles. En este caso, sólo queda el recurso de teclear.

Datos privados confidenciales en el puesto de trabajo

Un tema particularmente espinoso es el manejo de datos privados en el PC de la empresa. En primer lugar, surge la pregunta de si el PC del trabajo, al igual que otras instalaciones de la empresa (fotocopiadoras, máquinas de fax, etc.), pueden ser utilizados para fines particulares. Esto es algo que debería estar claramente preceptuado en el reglamento de la empresa o en el contrato de trabajo. Si se prohíbe por norma cualquier tipo de uso privado, lo mejor sería respetarlo y dejarse en casa todo lo que pertenezca al ámbito particular. Así, tampoco habrá que preocuparse demasiado de tomar precauciones especiales. Pero si el empresario permite o tolera que a veces se emplee el equipamiento de la empresa para fines particulares, podrá aprovechar esa ventaja. ¿Para qué comprar un PC caro, si puede y le permiten resolver la correspondencia ocasional desde la oficina?

Pero si usted procesa y almacena datos privados en los equipos de la empresa, debería tomar precauciones especiales para protegerlos de las miradas, ya sean casuales o intencionadas, de los colegas curiosos. Al contrario de lo que ocurre con un PC privado, al ordenador de la oficina no sólo tiene acceso usted, sino también otros empleados. Y si cualquier día coge la baja, cuente con que algún compañero recurra a su PC para poder utilizar en su ausencia documentos importantes, por ejemplo. Para que en un caso así no hagan también la ronda por la empresa sus archivos privados, le recomendamos que tome medidas de precaución especiales.

Correo electrónico en el PC de la empresa

Una cuestión importante es, sin duda, los mensajes de correo electrónico privados. Si su jefe permite enviar e-mails personales a través de la infraestructura técnica de la empresa, podrá aprovecharse de esta ventaja aunque, en este caso, le recomendamos encarecidamente que separe la comunicación profesional de la privada. Así, si debe ausentarse, podrá pedir a un compañero que cuide de su buzón de correo del trabajo, mientras los mensajes privados permanecerán sin leer hasta que usted vuelva. Ahora bien, seguramente no es costumbre solicitar al empresario la concesión de una segunda dirección de correo electrónico privada, aparte de la profesional. Además, en este caso seguiríamos con el problema de que los mensajes privados estarían depositados en el ordenador de la

empresa, donde podrían ser leídos por los compañeros o los administradores del sistema.

Pero existe una alternativa sencilla y barata que usted podrá aprovechar si no sólo le permiten enviar correos electrónicos, sino también navegar por la Red: hágase con un apartado de correo electrónico gratuito que pueda consultar a través del navegador web. En el capítulo 7 presentamos algunos proveedores de esta clase de direcciones de correo electrónico gratuitas. Para el caso que nos ocupa (el correo electrónico privado a través del ordenador de la empresa) ofrecen muchas ventajas.

- Con un apartado de correo electrónico adicional y gratuito, puede separar limpiamente los mensajes privados de los profesionales. Si está de vacaciones o enfermo, podrá ceder a un compañero de trabajo el control sobre su buzón profesional sin que esto afecte a sus mensajes personales.
- Usted recibe para sus asuntos particulares una dirección de correo electrónico, totalmente independiente de la empresa. Esto ofrece la ventaja de que sus mensajes privados no entrarán en contacto con sus jefes. Así, nadie podrá acusarle de abusar de la empresa para cuestiones privadas. Por otra parte, no tendrá que temer que sus opiniones personales lleguen a conocimiento de su jefe.
- Como la dirección de correo está dentro de Internet y es consultada a través del navegador web, el mensaje no es almacenado localmente en un ordenador de la empresa (siempre que usted mismo no guarde los diferentes mensajes a nivel local como archivos). Por consiguiente, sus mensajes particulares no podrán ser leídos por sus compañeros aunque usted esté ausente.
- Si usted vigila que la comunicación a través de la dirección de correo de la Red se realice mediante conexiones seguras (vea el capítulo 3), ni siquiera los administradores del sistema de su empresa podrán investigar el contenido de sus mensajes privados. Como todos los datos se intercambian encriptados, es imposible que su comunicación sea "espiada".
- Y para concluir, aunque usted cambie de trabajo, mantendrá su dirección de correo electrónico privada, ya que esta es independiente de ordenadores o redes en concreto. Incluso estando de vacaciones, usted podrá bajarse sus mensajes en todo momento desde un cibercafé o en casa de algún conocido que tenga acceso a Internet.

Proteger de un modo seguro los datos privados

Los e-mails privados pueden ser protegidos eficazmente con un apartado de correo virtual en Internet, según hemos explicado más arriba. Otra cosa son los

datos que tienen que estar disponibles en forma de archivo para que pueda trabajar con ellos. Quizá tenga en ellos información confidencial que sus compañeros no deban saber bajo ningún concepto, como por ejemplo la correspondencia con su seguro de enfermedad o con un abogado que le represente en un pleito. O imagine que alguien da con la documentación que usted había preparado para solicitar trabajo en otra empresa y se la enseña a su jefe actual. Esta clase de datos jamás deberían almacenarse así como así en el disco duro del PC del trabajo, donde los pueden encontrar en cualquier momento los compañeros, ya sea accidental o intencionadamente. A priori, lo mejor es guardar estos datos sólo en disquetes que podrá llevarse a casa o, al menos, dejar en lugar seguro. De este modo, también protegerá sus datos de que otro los borre por error o los machaque al hacer un mantenimiento.

TRUCO

No almacene los datos privados en las unidades de la red

Evite siempre guardar archivos privados confidenciales en las unidades de la red. Por un lado, estarían al alcance de todos los demás empleados y podrían ser descubiertos por casualidad o con intención. Según el sistema de red, estos archivos no tendrán más que una protección mediocre, o quizá ninguna. Además, los contenidos de las unidades de una red suelen ser sometidos a medidas de seguridad automáticas. De este modo, usted pierde el control sobre sus datos, ya que aunque hubiera borrado el archivo en algún momento, su contenido será conservado como copia de seguridad y podría ser restaurado durante alguna recuperación. Por norma, almacene sus datos personales sólo en el disco duro local del PC de su oficina, donde los podrá controlar y donde no se hacen regularmente copias de seguridad automáticas.

Si no puede guardar sus datos en disquetes, por el mero hecho de que quizá sean demasiado extensos o porque su PC no disponga de unidad de disquetes (cosa que, por razones de seguridad, no es nada infrecuente), deberá renunciar a estos métodos sencillos y rudimentarios. En este caso, existe una alternativa para guardar sus archivos en el ordenador de la empresa y, aun así, proporcionarles seguridad. Encripte los archivos cuando acabe de trabajar con ellos. En el capítulo 7 le mostramos cómo encriptar mensajes de correo electrónico. También demostraremos que con un procedimiento de encriptación PGP no sólo se pueden codificar textos de correo electrónico, sino también cualquier archivo binario. Emplee un procedimiento de este tipo para guardar encriptados los datos confidenciales. Si necesita un archivo, desencríptelo y, cuando termine con él, vuelva a encriptarlo enseguida y borre del disco duro la versión descodificada. De este modo, aunque un compañero descubra que usted guarda documentos personales en el ordenador, no los podrá abrir ni ver su contenido.

6.5 Windows en la red: una combinación peligrosa

INFO

Peligroso agujero de seguridad en el uso compartido de archivos de Windows

Según se ha sabido hace poco, la función de Windows para compartir archivos tiene ya desde la versión 95 un agujero de seguridad que permite a los hackers acceder a los archivos compartidos en la red, aunque éstos vayan protegidos por contraseña. Por un error de programación, se puede limitar al primer byte la comparación durante la consulta de la contraseña. De este modo, la cantidad de contraseñas posibles queda reducida a 256 y puede ser verificada fácilmente con un programa sencillo. Podrá encontrar más información sobre este error, contenido en las versiones 95, 98 y ME del sistema operativo de Windows, en http://www.microsoft.com/technet/security/bulletin/fq00-072.asp. También podrá descargarse parches para solucionar el problema.

Frecuentemente, en las empresas grandes y también en las más pequeñas, los diferentes PC están interconectados en una red. Ésta enlaza físicamente todos los ordenadores conectados entre sí y permite el intercambio de datos. Esto ofrece una serie de ventajas en un entorno laboral. Se pueden intercambiar fácilmente documentos y archivos. También permite la comunicación electrónica entre los empleados, por ejemplo vía correo electrónico. Por último, una red facilita el uso conjunto de recursos costosos como pueden ser impresoras o unidades de almacenamiento. También el sistema operativo Windows 9x/ME viene de fábrica con una amplia serie de funciones de red. De este modo puede ser empleado dentro de una red en combinación con otros ordenadores con Windows, pero también con sistemas operativos totalmente diferentes.

Pero al emplear Windows en una red, también existe multitud de riesgos adicionales para la seguridad. Y es que una conexión de red nunca es una calle de dirección única. También puede brindar a intrusos no autorizados la oportunidad de ver archivos confidenciales, o de sabotear los ordenadores de la red. En este apartado vamos a explicar los talones de Aquiles que tiene el empleo de Windows en una red y enseñarle cómo usar Windows de un modo seguro como sistema operativo de red.

El uso compartido de archivos e impresoras

Una función de red muy importante de Windows es el uso compartido de archivos e impresoras. Permite compartir los recursos de un PC de Windows con otros ordenadores que se encuentren dentro de la misma red. Si, por ejemplo, un pequeño departamento sólo dispone de una impresora láser, ésta podría ser conectada a uno de los ordenadores del departamento, que ofrecería la impresora al resto de los equipos a través de la red. Esto permitiría a todos los demás

empleados imprimir en ella sus documentos desde sus PC. Desde el punto de vista técnico, este sencillo ejemplo de uso compartido de impresora es prácticamente inocuo. Aunque un hacker pudiera "desprotegerlo", como mucho obtendría la dudosa ventaja de poder imprimir sus documentos gratis en la impresora.

La cosa cambia cuando hablamos del uso compartido de archivos. Funciona según el mismo principio, pero en este caso no es una impresora lo que se comparte, sino carpetas del disco duro local de un PC (o también todo el disco duro) para poder acceder a ellas a través de una red. De este modo, cualquiera puede acceder a estas carpetas a través de la red como si las tuviera emplazadas en su propio disco duro. La finalidad de compartir archivos vuelve a ser el trabajo conjunto. Así, un empleado puede preparar en su disco duro local documentos de interés general, como tal vez planes de proyecto, directrices, especificaciones, etc., que otros podrán consultar. Como el acceso no tiene por qué ser sólo de lectura, sino puede ser igualmente de escritura, los documentos facilitados también podrían servir para fines organizativos, permitiéndose por ejemplo a todos los implicados en un proyecto que actualicen el plan de proyecto en cualquier momento.

Hasta aquí la parte práctica y útil. Pero el "reverso tenebroso" de compartir archivos siempre supone un riesgo nada desdeñable. A fin de cuentas, el recurso compartido es accesible a través de la red, es decir, cualquiera que tenga acceso a la red también podría llegar hasta los datos. Por eso, lo importante cuando se compartan archivos es que se empleen siempre las funciones de seguridad ofrecidas. Esto permite restringir el acceso para que sólo puedan entrar las personas autorizadas.

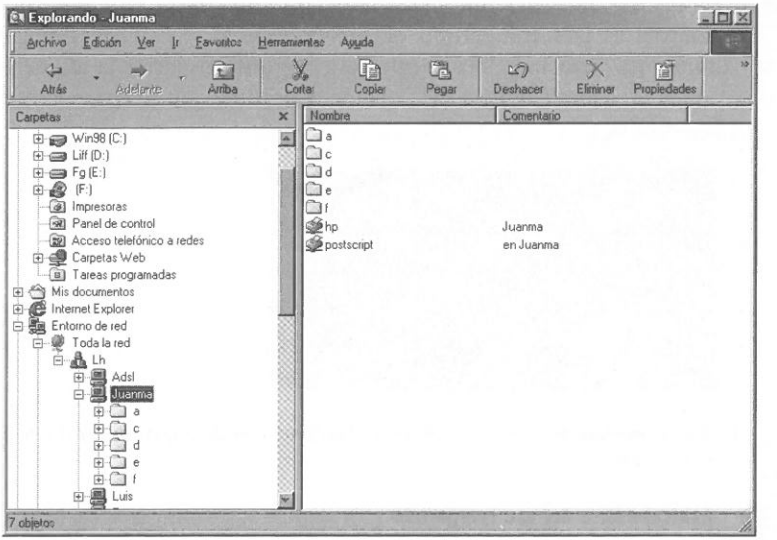
¿Qué archivos son compartidos?

Lo mejor será que compruebe por sí mismo si tiene ahora archivos compartidos en su PC y cuáles son. Para ello puede echar un vistazo en cualquier momento al entorno de red.

1. Abra el entorno de red haciendo doble clic sobre el icono del mismo nombre que aparece en el escritorio de Windows.

Con este icono puede abrir el entorno de red de su PC.

2. Abra ahora una a una las subcarpetas del entorno de red hasta que llegue al icono de su propio ordenador. Aquí encontrará las carpetas que estén compartidas en ese momento para un acceso desde la red. Además, en la parte derecha también aparecen junto a las carpetas las impresoras que puedan estar siendo compartidas.



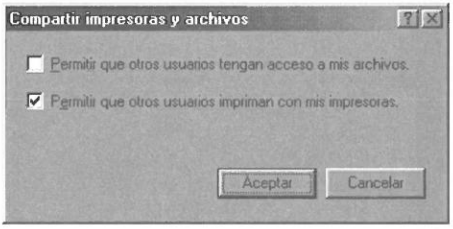
Así se comprueban los recursos que tiene compartidos en su PC en un momento determinado.

Desactivar totalmente el uso compartido de archivos e impresoras

La mejor protección contra el uso ilícito de las funciones para compartir es no utilizarlas en absoluto. Si puede y quiere renunciar completamente a esta funcionalidad, lo mejor sería que la desactive del todo. Así evitaría con suma eficacia un acceso ilícito a sus datos. Windows permite elegir con absoluta independencia entre desactivar el uso compartido de archivos y el de impresoras. Por consiguiente, podrá compartir sin reservas las impresoras, que prácticamente no suponen ningún peligro, mientras desactiva por completo el arriesgado acceso compartido a archivos.

1. Para controlar las funciones de uso compartido de la red Windows, abra *Inicio/Configuración/Panel* de control y haga doble clic sobre icono *Red*.
2. Aquí encontrará el botón *Compartir archivos e impresoras*, que le permitirá abrir un cuadro de diálogo especial para esta función.
3. La opción *Permitir que otros usuarios tengan acceso a mis archivos* controla el uso compartido de archivos. Si usted no quiere compartir sus carpetas y archivos locales para que otros usuarios accedan a ellos a través de la red, debería desactivar esta opción.

4. La opción *Permitir que otros usuarios impriman con mis impresoras* controla el uso compartido de las impresoras. Si quiere compartir una impresora conectada localmente para que otros usuarios la utilicen a través de la red, debería activar esta opción. Confirme con *Aceptar* la nueva configuración.



Estas opciones le permiten controlar las funciones de uso compartido de archivos e impresoras.

TRUCO

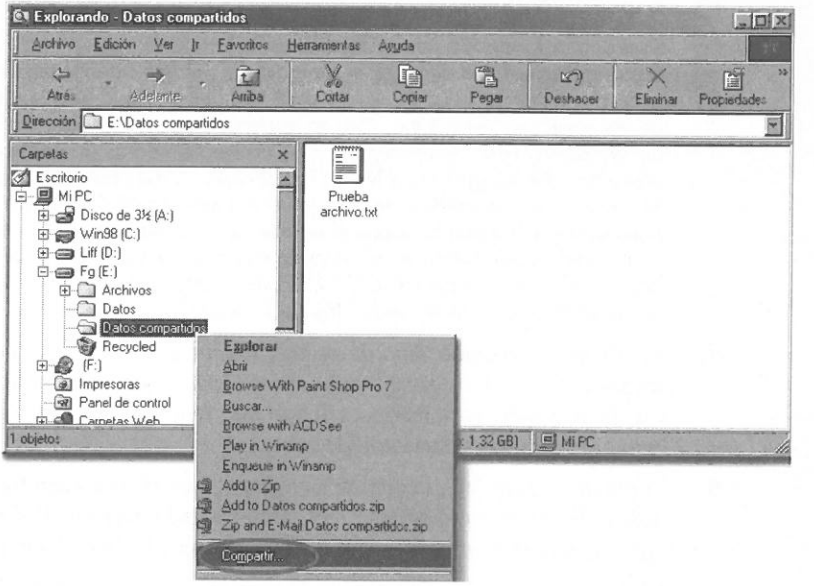
Control básico del uso compartido

En principio, las opciones descritas antriormente suponen sólo un control básico de la función de uso compartido que ofrece Windows. Si, por ejemplo, activa la utilización compartida de impresoras, esto no significa que ahora todas las impresoras de su PC conectadas localmente puedan ser compartidas de modo automático. Para ello deberá compartir expresamente cada impresora. Las opciones que hemos descrito sólo controlan la función básica, por lo que resultan especialmente indicadas para desactivar eficazmente todo uso compartido.

Compartir datos en la red de un modo seguro

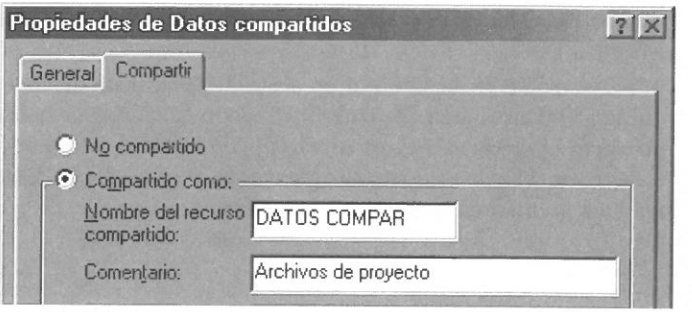
Si usted ahora ha decidido compartir determinados datos a través de la red, debería tener cuidado de emplear correctamente las funciones de seguridad disponibles para ello, de modo que los datos sólo puedan ser leídos por los que tengan autorización. De lo contrario, un atacante podría abusar de esa ventaja. Si únicamente existe un acceso para lectura, se podrían ver y copiar los archivos y documentos existentes. Pero si también se pudiera acceder con permiso de escritura, existe la posibilidad de modificar furtivamente los datos o infiltrar otros archivos, introduciendo tal vez en su ordenador virus o troyanos.

1. Para compartir una carpeta, arranque en primer lugar el Explorador de Windows y muestre la carpeta.
2. Ahora haga clic con el botón derecho del mouse sobre el nombre de la carpeta para desplegar el menú contextual de ese directorio. Seleccione la opción *Compartir*.



Encontrará la función de uso compartido en el menú contextual del Explorador de Windows.

3. Active primero la opción *Compartido como*, con la que configurará el acceso compartido a esa carpeta. Como *Nombre del recurso compartido*, Windows propone automáticamente los nombres de las carpetas. Pero puede elegir aquí cualquier otra denominación. Además, puede introducir un comentario, que aparecerá en el entorno de red correspondiente a esa carpeta. Ayudará a sus compañeros de trabajo a encontrar con más rapidez los datos buscados.



Active primero el acceso compartido, elija un nombre y, según el caso, un comentario.

TRUCO

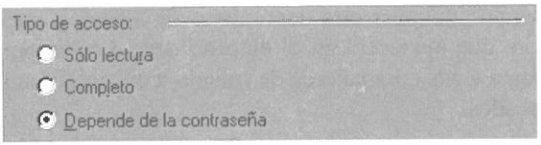
El truco del $

Un truco muy sencillo para dar nombre a la carpeta compartida puede hacer bastante segura esa utilización compartida. Añada al final del nombre de acceso compartido el símbolo especial $. Eso hará que la carpeta compartida no figure en la relación. Esto es aplicable por ejemplo al entorno de red de Windows, pero también para muchas herramientas de análisis de redes, como las que les gusta emplear a los hackers. Sigue existiendo la posibilidad de acceder a una unidad de red que haya sido ocultada de esta manera, pero sólo para quien conozca el nombre exacto de uso compartido. En resumen, si en nuestro ejemplo empleáramos en lugar de *DATOS DE RED* el nombre de uso compartido *DATOS DE RED$*, ocultaríamos esta carpeta liberada y quedaría sólo al alcance de "los de la casa".

4. Ahora, en el apartado *Tipo de acceso* habrá que decidir cómo deberá ser el acceso a los archivos compartidos. *Sólo lectura* permite acceder a los archivos de la carpeta para leerlos, aunque esto regirá para todos los usuarios de la red sin ninguna restricción de acceso.

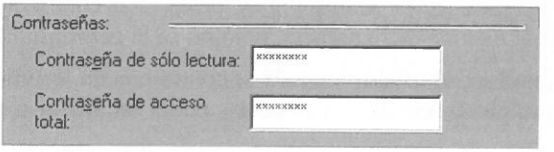
5. Lo mismo ocurre con la opción *Completo*, que en este caso todos los usuarios de la red no sólo podrán leer, sino también escribir. Por lo tanto, esta opción es la más insegura y no resulta recomendable en ningún caso.

6. Mucho más segura es la variante *Depende de la contraseña*. En este caso, se pedirá la contraseña a cada usuario que quiera acceder a los archivos compartidos. En función de esa contraseña, se le permitirá sólo la lectura o también la escritura. Esta configuración es la más segura y debería ser seleccionada en un caso normal.



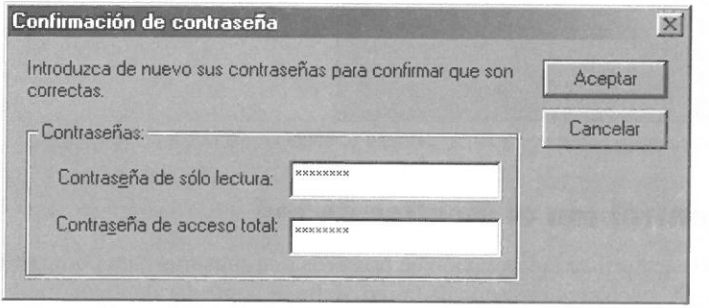
Elija si quiere restringir el acceso a los archivos compartidos y cómo deberá ser esa restricción.

7. Si previamente se decidió por un acceso dependiente de contraseña, introduzca ahora en el área *Contraseñas* las correspondientes palabras clave. Si un usuario introduce la *Contraseña de sólo lectura*, sólo se le permitirá leer el archivo. Si por el contrario conoce la contraseña de lectura/escritura, también podrá modificar y guardar archivos.



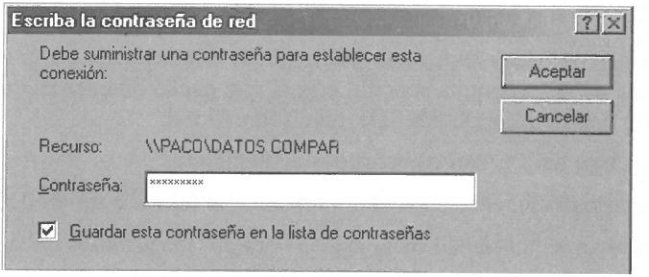
Introduzca las contraseñas para acceder a los datos compartidos.

8. Para finalizar la compartición de la carpeta con la configuración elegida, haga clic en *Aceptar*. Después, deberá repetir la introducción de las contraseñas para evitar errores de mecanografía.



Por razones de seguridad, hay que repetir la introducción de las contraseñas.

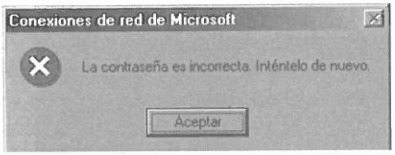
A continuación, echando un vistazo al entorno de red, podrá verificar si está la nueva carpeta compartida (salvo que usted hubiera añadido al nombre un $, según lo explicado; en este caso, la carpeta no aparecería). Si ahora otro usuario de red pretende acceder a una carpeta compartida que haya sido protegida de esta manera, primero tendrá que enfrentarse a una petición de contraseña.



Para acceder a una carpeta de red protegida por contraseña, el usuario debe introducir la palabra clave.

En función de la contraseña introducida, se permitirá el acceso a la carpeta de red en las siguientes condiciones:

- Si el usuario introduce la contraseña de protección contra escritura, sólo podrá leer el contenido de la carpeta, pero no se le permitirá modificarlo.
- Si, por el contrario, el usuario conoce la contraseña de lectura y escritura, se le permitirá pleno acceso a la carpeta y podrá modificar o añadir archivos.
- Si el usuario ha introducido una contraseña totalmente equivocada, le será denegado el acceso a la carpeta de red hasta que teclee la palabra clave correcta.



Sin la contraseña correcta, se deniega el acceso a los datos compartidos.

Control con el Monitor de red

Si usted utiliza la liberación de archivos e impresoras para compartir recursos de su PC con otros usuarios de la red, debería controlar de algún modo quién aprovecha esos recursos. Por una parte, esto fomenta la seguridad, ya que usted sabe inmediatamente si ha accedido alguien que no tiene autorización. Por la otra, habría que vigilar que el uso compartido del PC en la red no sea utilizado en exceso. A fin de cuentas, el ordenador debe emplear parte de su rendimiento para contestar a las consultas desde la red, por lo que en esos momentos trabajará más despacio. Si esto se convierte en su estado permanente, sería recomendable replantearse la política de uso compartido en la red y quizá preparar un servidor dedicado expresamente a estas tareas.

Para vigilar las actividades realizadas desde la red, Windows aporta su Monitor de red. Se trata de un programa sencillo con el que puede obtener en cualquier momento todo tipo de información relevante sobre la red:

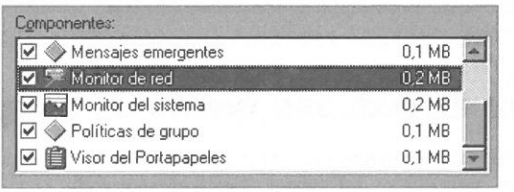
- ¿Qué recursos del PC son compartidos actualmente?
- ¿Qué usuarios están enlazados ahora mismo con mi PC a través de la red?
- ¿Qué archivos están siendo manejados ahora por los usuarios de la red?

Aparte de estas cuestiones meramente informativas, el supervisor de la red también ofrece funciones administrativas sencillas. Permite anular un acceso compartido con un simple clic del mouse, o desterrar del propio PC a los usuarios sospechosos. Encontrará el Monitor de red en *Inicio/Programas/Accesorios/Herramientas del sistema/Monitor de red.*

Instalar posteriormente el Monitor de red

Si durante la instalación de Windows el Monitor de red no se hubiera instalado, podrá hacerlo manualmente:

1. Abra el Panel de control de Windows con *Inicio/Configuración/Panel de control* y, una vez allí, haga doble clic en el icono *Agregar o quitar programas.*
2. En la ventana *Propiedades de Agregar o quitar programas*, acceda a la pestaña *Instalación de Windows*, donde se mostrarán los detalles de los programas del sistema instalados.
3. Haga doble clic sobre la categoría *Herramientas del sistema* y active la opción *Monitor de red.*



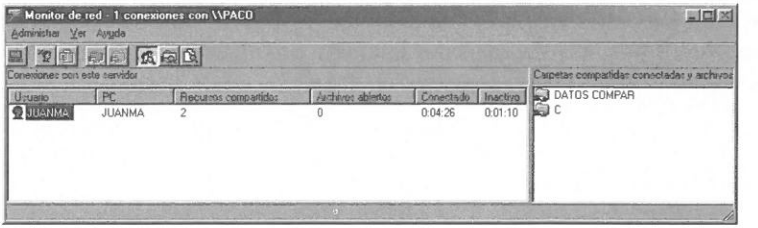
Active Monitor de red para instalarlo complementariamente.

4. Confirme con *Aceptar* la instalación del *Monitor de red.*
5. Si lo considera oportuno, acepte la invitación del programa de instalación e inserte el CD-ROM de instalación de Windows.

Con esto quedará instalado el *Monitor de red.* A partir de ahora, podrá acceder a él desde *Inicio/Programas/Accesorios/Herramientas del sistema/Monitor de red.*

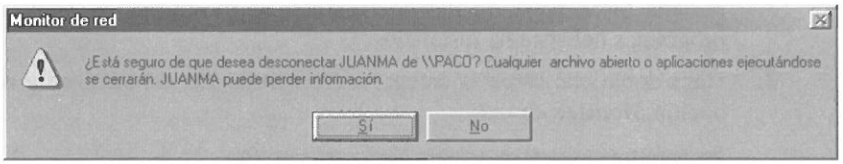
El Monitor de red en acción

Cuando arranque el Monitor de red, mostrará los usuarios que se hayan conectado en ese momento a su PC. Para cada usuario, le dará el nombre de usuario y el ordenador desde donde se iniciara la sesión. Por lo tanto, si conoce un poco su red local, podrá averiguar rápidamente quién es esa persona.



El Monitor de red le muestra de un vistazo los usuarios que están conectados en su PC en ese momento.

Si uno de los usuarios le parece sospechoso o si desea interrumpir el enlace por alguna otra razón, puede desconectar al usuario. Para ello, márquelo en la lista y seleccione *Administrar/Desconectar usuario*, o emplee el icono *Desconectar usuario* situado en la barra de herramientas. Confirme la siguiente consulta de seguridad con *Sí*. Pero cuando lo haga tenga muy en cuenta que al ser desconectado, ese usuario podrá perder datos, por lo que este remedio sólo debería ser empleado si las circunstancias hacen sospechar un acceso ilícito, no para tomar el pelo a algún compañero de trabajo.



Confirme la consulta de seguridad para desconectar a un usuario de su ordenador.

Los protocolos de red: una fuente de peligros

Para ser un sistema operativo concebido principalmente con miras a su uso en entornos sencillos de oficina o del hogar, las funciones de red de Windows 9x/ME son asombrosamente flexibles y eficientes. De modo parecido a lo que ocurre con su hermano mayor Windows 2000, en un ordenador se pueden ejecutar en paralelo multitud de componentes y protocolos de red. Así, por ejemplo, es posible conectar un ordenador a una red mediante una tarjeta de red y, simultáneamente, conectarse a Internet vía módem o adaptador RDSI. También se pueden montar dos tarjetas de red en un PC con Windows, para emplearlo por hardware en dos redes diferentes. Por el lado del software, el PC con Windows puede emplear al mismo tiempo varios protocolos de red diferentes, como por ejemplo el protocolo de Internet TCP/IP y el protocolo de uso compartido de archivos e impresoras explicado anteriormente.

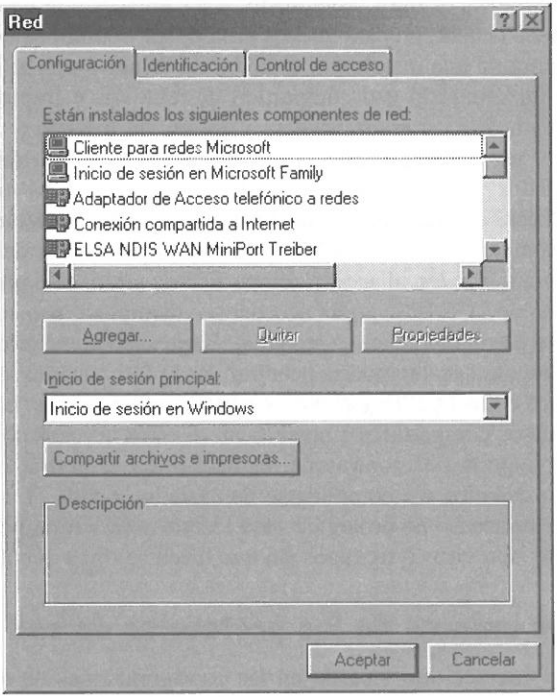
Pero es justo en esta flexibilidad y versatilidad donde también están su gran debilidad y peligro. El trabajo conjunto de diferentes componentes y protocolos de red tiene lugar mediante lo que llamamos enlaces. Por ejemplo, para que se pueda producir una conexión a Internet, el Adaptador de Acceso telefónico a redes (el responsable del establecimiento técnico de la conexión a través de la línea telefónica) es enlazado con el protocolo TCP/IP (que se encarga del transporte de los paquetes de datos por Internet). Sin un enlace entre estos dos, no se puede producir ningún intercambio de datos.

Por desgracia, Windows es muy "aficionado" a los enlaces y le gusta establecer todos los que pueda cuando prepara nuevos protocolos y componentes. Un ejemplo sencillo: si durante una instalación estándar de Windows es hallada una tarjeta de red, se implantará el uso compartido de archivos e impresoras. Hasta aquí, todo está bien. Pero si ahora conecta a ese PC un módem o un adaptador RDSI para entrar en Internet, también será instalada la tarjeta de red para la transmisión de datos y del protocolo TCP/IP (según lo descrito más arriba), y Windows establecerá enlaces entre todos los componentes. Es decir, el protocolo TCP/IP también será vinculado a la tarjeta de red y, a través del *Adaptador de Acceso telefónico a redes*, al acceso compartido de archivos e impresoras. De modo que a través de TCP/IP se podrá acceder por ejemplo al uso compartido de archivos, previsto en realidad para la red local. Expresado con claridad, esto significa lo siguiente: un atacante podría penetrar desde Internet en su ordenador y, a través del enlace entre TCP/IP y el uso compartido de archivos, hacerse con el acceso a los recursos compartidos a nivel local. Si estos accesos compartidos ni siquiera van protegidos por contraseña, el hacker hasta podría consultar los archivos de su ordenador sin complicarse demasiado la vida. Y si a lo mejor había concedido un acceso no protegido para lectura y escritura, podría infiltrar en su PC archivos con virus o troyanos sin que usted se diera cuenta.

Verificar los enlaces de los protocolos de red

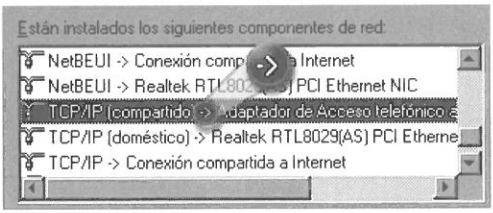
Para evitar estas interacciones ocultas en las configuraciones de red de su PC bajo Windows, le recomendamos que compruebe sin falta los enlaces de red. La regla empírica a aplicar sería: cuantos menos enlaces haya, mejor. Naturalmente, ciertos enlaces son inevitables si se pretende que funcione la red, pero bajo ningún concepto deberían permitirse algunas configuraciones si queremos evitar que peligre la seguridad de nuestros datos.

1. Para verificar la configuración de red de su PC, primero acceda a *Inicio/Configuración/Panel de control*, donde deberá abrir el icono *Red*.



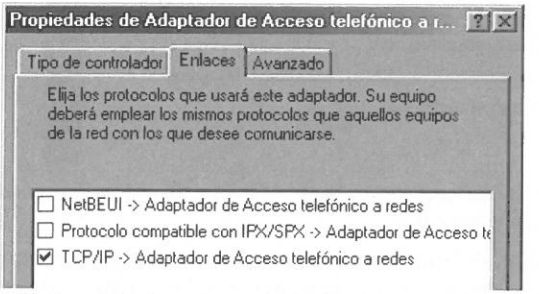
En las propiedades de la red encontrará todos los componentes y protocolos de red con sus enlaces.

2. Hallará en la pestaña *Configuración* una relación completa de todos los componentes de red instalados. Encontrará adaptadores como el *Adaptador de acceso telefónico a redes*, al igual que protocolos como *TCP/IP*, o servicios y clientes como por ejemplo el *Cliente para redes Microsoft*. Además, también habrá una entrada para cada enlace entre dos componentes de red. Lo reconocerá por la flecha ->, que simboliza el enlace entre dos componentes.



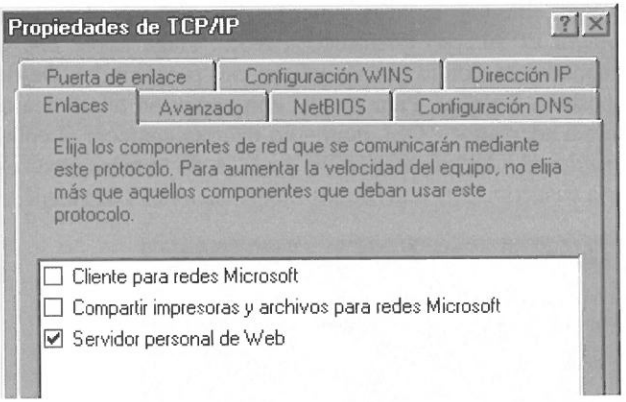
Una flecha simboliza el enlace entre dos componentes de red, en este caso, los del protocolo TCP/IP.

3. Si quiere eliminar enlaces innecesarios, debería dedicarse primero al Adaptador de Acceso telefónico a redes. Haga doble clic en la entrada correspondiente, con lo que visualizará sus propiedades. Desde allí, cambie a la pestaña *Enlaces*. Para un PC con conexión telefónica a Internet vía módem o adaptador RDSI, aquí sólo debería aparecer el enlace *TCP/IP -> Adaptador de Acceso telefónico a redes*. Si hubiera otros enlaces, quizá debería desactivarlos. Guarde las modificaciones con *Aceptar*.



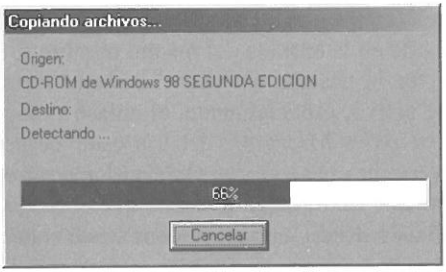
Elimine todos los enlaces del Adaptador de Acceso telefónico a redes, excepto TCP/IP.

4. De vuelta a la ventana *Red*, debería observar más de cerca el enlace *TCP/IP -> Adaptador de Acceso telefónico a redes*. Para ello, visualice sus propiedades haciendo doble clic en la entrada del mismo nombre y, en la siguiente pantalla, abra otra vez la pestaña *Enlaces*. Lo mejor sería que aquí no hubiera ningún enlace activo, especialmente, el enlace *Compartir impresoras y archivos para redes Microsoft* debería estar desactivado, a ser posible. Sólo puede convenir el enlace con el *Servidor personal de Web*, si es que existe. Pero, en este caso, tenga presente que el *Servidor personal de Web* podrá ser utilizado desde Internet mientras esté conectado. Vuelva a guardar los cambios con *Aceptar*.



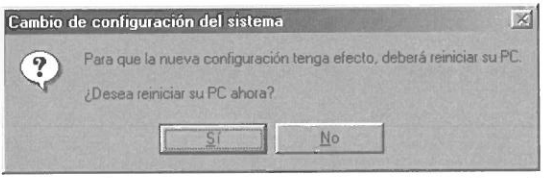
A ser posible, TCP/IP tampoco debería tener ningún enlace aparte del Adaptador de Acceso telefónico a redes.

5. A continuación, deberá hacer otra vez clic en *Aceptar* en la ventana *Red* para guardar definitivamente la nueva configuración. Después, Windows actualizará la configuración de red. Quizá sea necesario insertar el CD-ROM de instalación para que se puedan instalar los archivos necesarios.



Windows actualiza la configuración de la red con los nuevos cambios.

6. Después, será necesario reiniciar Windows para que la nueva configuración pueda ser actualizada. Sólo después del reinicio entrarán en vigor la nueva configuración segura.



Por norma, después de haber modificado la configuración de la red hay que reiniciar el ordenador.

El Servidor de acceso telefónico a redes como vía de invasión

Si su PC va equipado con un módem o una tarjeta RDSI, puede establecer a través de la línea telefónica una conexión con otros ordenadores o con Internet. Pero esta vía no es una carretera unidireccional. Otros ordenadores pueden utilizar igualmente su módem o su tarjeta RDSI para establecer una conexión con su ordenador y, por ejemplo, transmitirle archivos. Para que esto funcione, en su ordenador deberá ejecutarse un programa especial, el Servidor de acceso telefónico a redes, que recibe las llamadas de otros ordenadores y prepara los archivos.

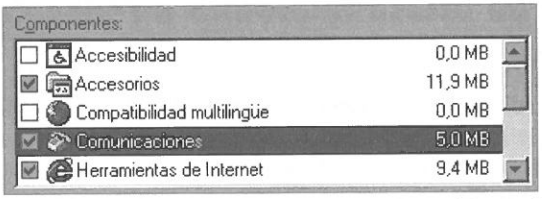
Si facilitamos a otras personas el acceso telefónico a nuestro ordenador, corremos algunos riesgos. Por ejemplo, hay que controlar con exactitud quién puede utilizar ese acceso. Si no hay ninguna restricción para iniciar una sesión, cualquiera que se haya hecho de algún modo con nuestro número de teléfono, podría aprovecharse de ese acceso.

Windows aporta su propio Servidor de acceso telefónico a redes. Si quiere renunciar a sus servicios, lo mejor será que lo desactive para minimizar cualquier riesgo. A continuación vamos a explicarle el modo más fiable de desactivarlo. Además, le describiremos cómo podrá configurar el Servidor de acceso telefónico a redes con seguridad si quiere ofrecer servicios de servidor.

Desinstalar el Servidor de acceso telefónico a redes

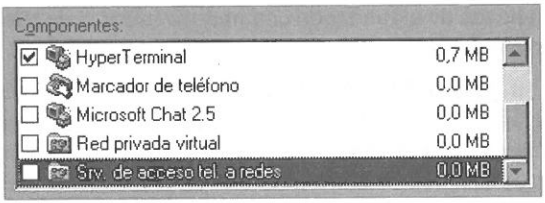
Si no quiere utilizar el Servidor de acceso telefónico a redes, lo mejor será desinstalarlo. Al hacerlo, este componente de software será eliminado totalmente de su ordenador, de modo que ya no supondrá ningún riesgo. Esta desinstalación es recomendable para la gran mayoría de usuarios, con lo que nos surge la pregunta de por qué Microsoft hace instalar por omisión el Servidor de acceso telefónico a redes.

1. Para desinstalarlo, abra en primer lugar *Inicio/Configuración/Panel de control* y acceda a *Agregar o quitar programas.*
2. Aquí, cambie a la pestaña *Instalación de Windows.* Tras un breve tiempo de espera, aparecerá la configuración de software actual de Windows.
3. Haga doble clic sobre *Comunicaciones* para abrir sus propiedades.



Con un doble clic en Comunicaciones mostrará las opciones de comunicación de datos de Windows.

4. Ahora aparecerá una relación de los componentes de enlace, donde podrá ver los que estén instalados en ese momento. En segundo lugar verá el Servidor de acceso telefónico a redes. Si éste lleva una marca a la izquierda, significará que está instalado. Para desinstalarlo, elimine la marca con un simple clic del mouse.



Así desinstala usted el Servidor de acceso telefónico a redes de Windows.

5. A continuación, haga dos veces clic en *Aceptar* para desinstalar el Servidor de acceso telefónico a redes.

Después de esto, podrá comprobar en la ventana de propiedades de Red que el servidor de teletransmisión de datos y sus configuraciones realmente han desaparecido (vea también el siguiente apartado).

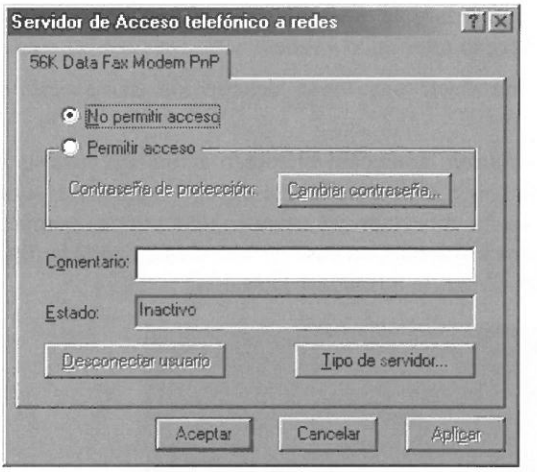
Configure el servidor de acceso telefónico a redes con seguridad

Si usted no quiere renunciar al servidor de acceso telefónico a redes, al menos debería configurarlo de modo que no pueda ser empleado ilícitamente. El servidor ofrece algunas funciones de seguridad para eso, que sólo hay que ajustar correctamente.

1. Abra en el puesto de trabajo la carpeta *Acceso telefónico a redes* (dentro de la carpeta Mi PC).
2. Seleccione *Conexiones/Servidor de Acceso telefónico a redes* para abrir la pantalla de configuración del servidor.
3. En la ventana del *Servidor de Acceso telefónico a redes* encontrará una pestaña para cada módem y cada tarjeta RDSI que haya instalado. Podrá deci-

dir individualmente para cada uno de estos aparatos si debe permitirse una conexión telefónica. Si para uno de los dispositivos hay instalado más de un controlador, encontrará para cada uno su propio registro, por lo que la configuración podría resultar un poco confusa.

4. Si quiere bloquear las funciones de servidor para uno de esos dispositivos, asegúrese de que esté activada la opción *No permitir acceso*. Si desea eliminar del todo el *Servidor de Acceso telefónico a redes*, verifique si esta opción está desactivada en TODOS los dispositivos.



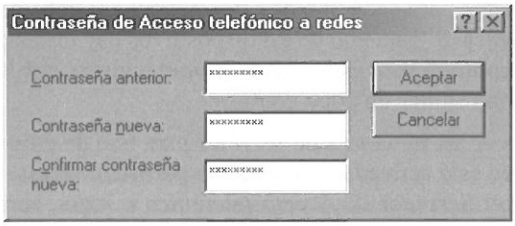
Así se puede desactivar el Servidor de Acceso telefónico a redes.

5. Si desea permitir la conexión telefónica a través de uno de los dispositivos, active la opción *Permitir acceso*.

6. Esto activará el botón Cambiar contraseña. Haga clic sobre él para proteger con una palabra clave el acceso por conexión telefónica. Todo aquel que se conecte a su ordenador a través del Servidor de Acceso telefónico a redes, deberá conocer esta contraseña.

7. En la ventana *Contraseña de Acceso telefónico a redes*, introduzca en primer lugar la contraseña anterior. Si hasta ahora aún no había empleado ninguna, deje ese campo de entrada en blanco.

8. En el campo *Contraseña nueva*, introduzca la palabra clave para el acceso y repita la entrada en el campo *Confirmar contraseña nueva*. Así evitará errores de mecanografía. En cuanto a la elección de una palabra clave segura, le recomendamos que tenga en cuenta los consejos del capítulo 2.1.

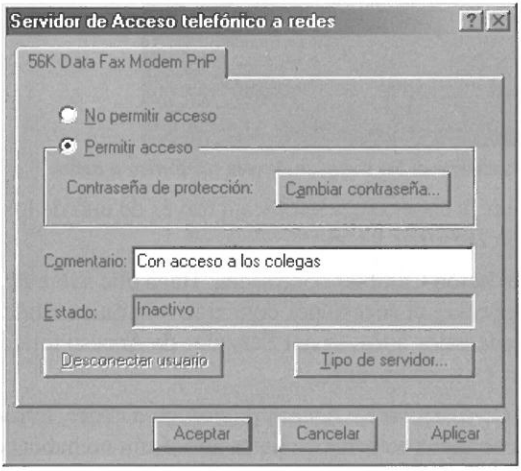


Introduzca una contraseña para el control de acceso a su ordenador.

9. Con *Aceptar* guardará la nueva palabra clave y volverá al menú del Servidor de Acceso telefónico a redes.

10. Aquí podrá introducir una breve descripción del acceso en el campo *Comentario*.

11. En el campo *Estado* aparecerá el estado actual del acceso por conexión telefónica. Si nadie está usando ese acceso, aparecerá aquí el mensaje *Inactivo*. Si se ha conectado un usuario, verá en este campo información detallada sobre él. Además, en caso de necesidad, con el botón *Desconectar usuario* podrá obligarle a finalizar la sesión.



Un acceso correctamente configurado, con protección por contraseña.

7 E-mail: arma, fuente de información y medio de comunicación

7.1 El e-mail como arma – ataques por correo electrónico 365
Remitente desconocido – borrar las huellas del e-mail 365
Bajo bandera falsa – falsificar el remitente del e-mail 370
Bombas virtuales – paralizar sistemas mediante correo electrónico 375
Virus de e-mail, ¡no, gracias! – la configuración del programa de correo electrónico 381

7.2 El correo electrónico como fuente de información – los riesgos de la correspondencia electrónica 390
Postales electrónicas – por eso las puede leer cualquiera 390
¿Cuánto se espía realmente? 394
Contramedidas: encriptar los mensajes 397
Así se revientan las claves 402

7.3 Lectores encubiertos, ¡no, gracias! – encriptar un e-mail con PGP 404
Las herramientas de PGP 404
Distribuir las claves propias PGP 412
Incluir claves públicas 415
Leer mensajes encriptados 420
Firmar mensajes 421
Emplear PGP con cualquier aplicación 424
La encriptación de archivos adjuntos 429
¿Hasta qué punto es fiable PGP? 430
S/MIME – la alternativa de pago 430

7.4 Ocultar en lugar de desencriptar – protección mediante esteganografía 433
La idea: ocultar información confidencial entre masas de datos 434
Volver visibles los datos ocultos 440

7.5 Freemailer – gratuitos, pero no exentos de peligro 443
GMX & Co. – servicios de correo electrónico a través de la Red 444
Más vale prevenir – las reglas más importantes a seguir con los servicios de freemail 446
Una dirección para cada asunto – aprovechar las direcciones gratuitas de correo electrónico 448

En pocos años el e-mail, el correo electrónico de Internet, ha conseguido imponerse como nuevo medio de comunicación en todos los ámbitos de la vida. Tarde o temprano eclipsará del todo al correo clásico por carta. Son demasiadas las ventajas que ofrece esta forma de comunicación puramente electrónica. Una velocidad vertiginosa unida a unos costes incomparablemente bajos, más el hecho de tener al alcance cualquier parte del mundo, convierten al correo electrónico en el medio de comunicación del futuro.

Es comprensible que, con tantas ventajas, no nos guste plantearnos las posibles desventajas y los problemas que acompañan al uso de los e-mail. De hecho, el correo electrónico no sólo puede ser un medio de comunicación fiable y cómodo, sino también una fuente de información para terceros no autorizados. Como el correo electrónico se basa en el sistema abierto que es Internet, los mensajes electrónicos son transmitidos prácticamente sin protección a través de los ordenadores y las redes de todo el mundo. Quien quiera leerlos, quizá para ejercer el espionaje o vigilar a una víctima potencial, podrá hacerlo con escaso esfuerzo técnico. Que los servicios secretos estatales ya lo hacen sistemáticamente es un hecho, que es puesto en tela de juicio con escasa convicción.

INFO

¿Husmean los servicios secretos la comunicación mundial?

Casi una leyenda ya entre amigos y enemigos del servicio secreto es el sistema Echelon. Se dice que es uno de esos proyectos de espionaje a gran escala. Está colocado en varios nodos de intercambio importantes de las redes de comunicación mundiales, donde inspecciona los mensajes en tránsito y los filtra mecánicamente. Durante mucho tiempo se puso en tela de juicio su existencia porque, naturalmente, los organismos oficiales nunca la reconocieron. Pero ahora se puede considerar a Echelon como un hecho consumado. Lo más chocante: Echelon es explotado bajo control de los Estados Unidos y no es, en absoluto, una organización internacional. ¿De verdad irán dirigidas las escuchas ilegales sólo contra terroristas o traficantes de drogas, o también enfocarán alguna vez a empresas comerciales y autoridades de países "amigos"?

Más información sobre Echelon:

http://www.heise.de/tp/english/special/ech/

http://www.echelonwatch.org/

http://www.iptvreports.mcmail.com/ic2kreport.htm

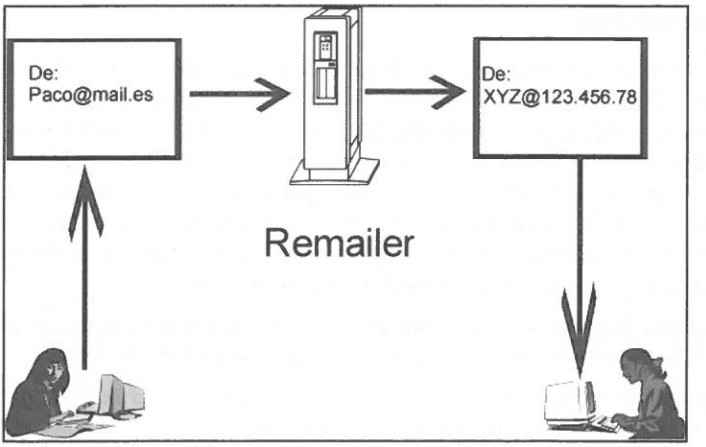
Sin embargo, el correo electrónico no sólo puede ser usado pasivamente como fuente de información. La arquitectura abierta de Internet permite, incluso, emplear los mensajes electrónicos como arma, para molestar y acosar a los usuarios, o llegar hasta a anular por completo a ordenadores y redes. Este capítulo trata de los aspectos relacionados con la seguridad de la comunicación electrónica por e-mail. Vamos a descubrir sus puntos débiles y revelarle a usted cómo proteger su información confidencial de cualquier ataque.

7.1 El E-mail como arma – ataques por correo electrónico

¿Un medio de comunicación como el correo electrónico puede considersrse como arma? ¿Cómo se come eso? El correo electrónico es comparado constantemente con la correspondencia clásica por carta, o incluso aclamado como sucesor de ésta. También se puede establecer un paralelismo entre el potencial de peligro de ambos. Por ejemplo, las cartas-bomba con explosivos son una herramienta terrorista que se emplea constantemente. Igualmente se puede causar daño con cartas falsificadas, o enviar anónimamente insultos o chantajes. Tampoco el correo electrónico es inmune a estos usos ilícitos, según vamos a explicar en las siguientes páginas.

Remitente desconocido – borrar las huellas del e-mail

¿Por qué tiene que llevar un e-mail siempre un remitente? Con el correo real, también se pueden enviar cartas anónimas por el sencillo procedimiento de omitir los correspondientes datos en el sobre. Cuando enviamos un e-mail eso no es tan sencillo, ya que los programas de correo electrónico normales insertan automáticamente nuestra dirección de e-mail como remitente. Aunque tampoco hace falta que digamos la verdad, cuando introduzcamos estos datos en la configuración. Pero por otra parte, quien crea que va a quedar en el anonimato con *usuario@senado.es*, está muy equivocado. Casi siempre, se pueden encontrar rápidamente en la cabecera del e-mail huellas sobre la verdadera identidad del remitente. Con este sistema engañará, como mucho, a los principiantes.



Así trabajan los remailer.

Si usted quiere permanecer de verdad en el anonimato puede emplear un servicio especial de Internet, lo que se denomina como *remailer*. Estos servidores especiales reciben los e-mail y los remiten al destinatario real, suprimiendo sin dejar rastro la dirección y cualquier otro dato que delate al remitente. El destinatario recibirá su e-mail desde una dirección inexpresiva y no tendrá (casi) ninguna oportunidad de descubrir al remitente real.

INFO

¿Hasta qué punto son fiables los remailer?

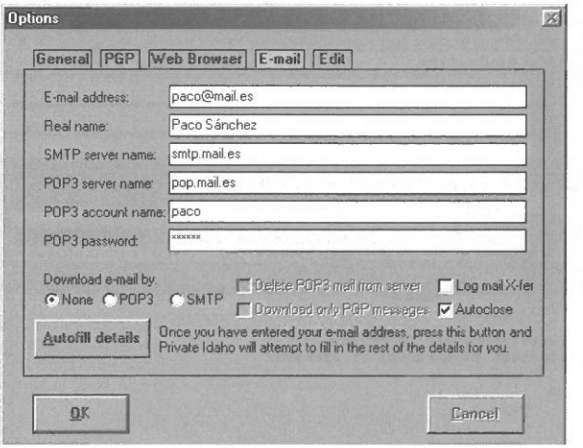
Los remailer son muy fiables. Aunque esto no debe hacernos pensar que podemos abusar de ellos para cualquier fin. Los mailing anónimos tienen, desde luego, su finalidad. Fueron desarrollados pensando, sobre todo, en aquellas personas, que no quieran darse a conocer cuando participen en determinados foros. Si, por ejemplo, el director de un instituto de enseñanza media rural pregunta en una lista de mailing especializada dónde se celebrará el próximo fin de semana en las cercanías una fiesta sadomasoquista, este e-mail podría llegar fácilmente a manos de sus colegas o alumnos. Por lo tanto, si quiere evitarse los problemas que le caerían encima, utilizará en lugar de eso un e-mail anónimo. De este modo conseguirá la información sin temor a represalias. No obstante, los servicios remailer no están pensados para la gente que quiera molestar, ofender, intimidar o chantajear a otros. Tampoco son nada apetecibles las personas que abusan de los e-mail anónimos para enviar correos basura. ¿Qué ocurre en estos casos? Muy sencillo: tan anónimo no es el servicio remailer. Si el operador advierte que su servicio ha sido usado fraudulentamente en algún caso concreto, puede averiguar a partir de sus archivos de registro quién era el remitente verdadero. En caso de delito, descubrirá a este remitente con toda seguridad. En todos los demás casos podemos confiar en la discreción de los remailer.

Private Idaho – convierta en anónima su comunicación

Si usted necesita comunicarse anónimamente a través de Internet, debería echar sin falta un vistazo al programa Private Idaho. Puede obtenerlo gratuitamente en http://www.lynagh.demon.co.uk/pidaho. Este programa le ofrecerá una interfaz cómoda para enviar e-mail anónimos. Antes de poder utilizarlo deberá configurarlo en su primera puesta en marcha. Para poder enviar sus e-mail, deberá configurarlo con los datos del servidor de correo saliente. Éstos deberían ser los mismos que tenga asignados en las categorías correspondientes de su programa de correo electrónico, que podrá consultar en caso de duda.

1. Cuando haga el primer arranque aparecerá automáticamente el menú de configuración de Private Idaho. Pase aquí a la pestaña *E-mail*.
2. En *SMTP server name:* indique el nombre del servidor de correo saliente, al que Private Idaho deba enviar sus mensajes.

3. En *POP3 server name:* teclee el nombre del servidor de correo entrante, donde Private Idaho deba recoger los mensajes que entren (suponiendo que usted quiera utilizar Private Idaho para eso).
4. Finalmente, en el campo *POP3 account name:* introduzca el nombre de usuario, con el que Private Idaho deba identificarse ante el servidor de correo entrante cuando establezca la conexión POP para recoger el correo. El programa pedirá siempre la correspondiente contraseña cuando establezca la conexión.
5. También podrá rellenar los demás campos, pero la información de éstos no es realmente necesaria para enviar mensajes anónimos. Guarde la información introducida con *OK*. Ahora, Private Idaho dispondrá de todos los datos requeridos para enviar los mensajes anónimos de usted.



Proporcione a Private Idaho los datos más importantes, para que usted pueda acceder al correo electrónico.

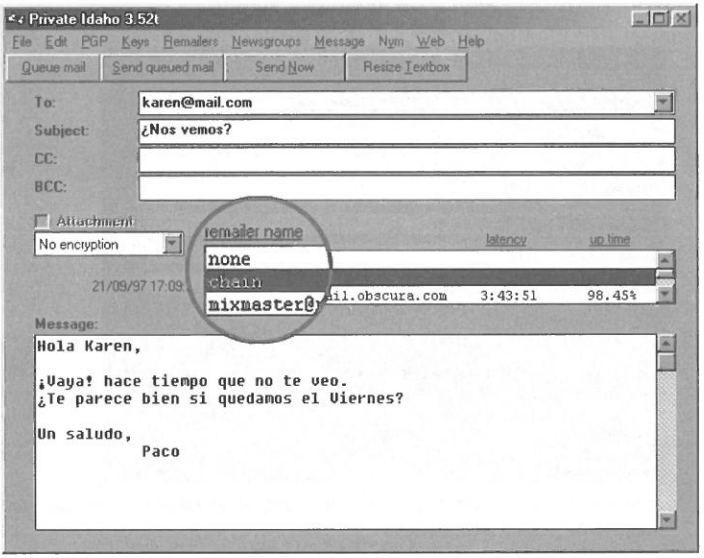
Así funciona – envíe un e-mail anónimo

La creación de un e-mail anónimo, en principio, no se diferencia de la redacción de cualquier otro mensaje. Teclee el texto que desee, teniendo cuidado de no revelar su identidad en algún punto que no sea la línea de remitente (por ejemplo con una firma).

1. Indique el destinatario en el campo *To:* e introduzca la línea de asunto en el campo *Subject:*. Si fuera necesario, en los campos *CC:* y *BCC:* hay espacio para otros destinatarios. Teclee en el cuadro de texto *Message:* el contenido del mismo.

2. El siguiente paso será seleccionar el remailer que deba convertir a su mensaje en anónimo. En el campo *remailer name*, dispone de varios servicios. En cada entrada de remailer, aparte del nombre encontrará también los datos correspondientes a *latency* (el tiempo de latencia que necesita el remailer para reenviar su mensaje) y *up time* (lo fiable que es on-line el servidor del remailer).

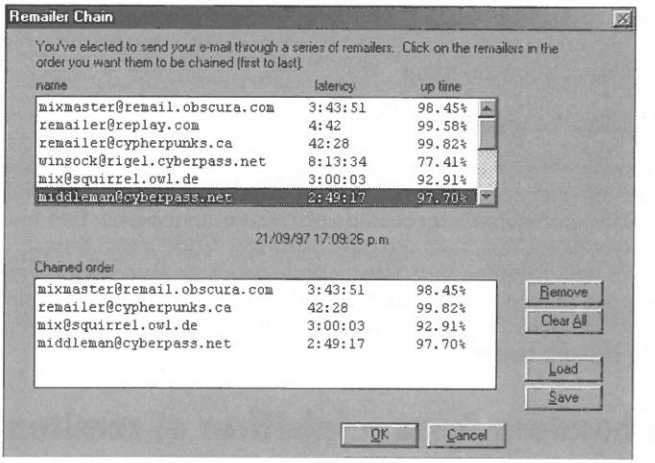
3. Si usted quiere ir a lo seguro, decídase por *chain*. Entonces, su mensaje será enviado a través de varios remailer y cada uno de ellos lo enmascarará a su vez. Este camuflaje múltiple hace prácticamente imposible identificar al remitente original. Aunque como contrapartida el transporte del mensaje podría llevar algo más de tiempo.



Cree primero el mensaje y seleccione el remailer.

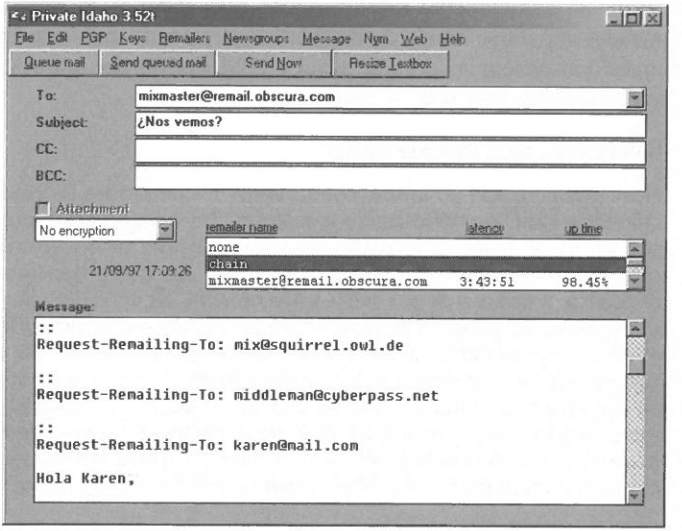
4. Si quiere preparar el mensaje para su envío anónimo, active la función *Message/Append Info*.

5. Si previamente había seleccionado el modo *chain*, ahora deberá establecer la cadena de servidores remailer que deban camuflar sucesivamente su mensaje. En el cuadro de lista superior encontrará todos los servidores disponibles. Con doble clic trasladará al cuadro de lista inferior uno o varios servidores. También puede elegir varias veces un mismo servidor, que transmitirá repetidamente el mismo mensaje enmascarado.



Seleccione los servidores remailer a través de los cuales deba ser enmascarado el mensaje.

6. Una vez concluida la selección confírmela con *OK*. Private Idaho preparará el mensaje para ser enviado anónimamente. Después de esto tendrá un aspecto algo extraño, pero eso es normal. Para cada uno de los remailer implicados se insertará una entrada especial en el comienzo del mensaje. Como destinatario del mensaje anónimo, será insertado en la línea *To* el primer (o único) servidor remailer de la cadena.



Este es el aspecto que tiene el mensaje preparado para el envío anónimo.

7. Para enviar ahora el mensaje anónimamente haga clic sobre el botón *Send*. Private Idaho lo enviará a su servidor de correo saliente, desde donde iniciará su camino anónimo.

TRUCO

Actualizar los remailers

Los remailer casi siempre son ofertas gratuitas, que organizaciones o particulares ofrecen por idealismo. Muchas veces estas ofertas no pueden ser mantenidas, por ejemplo a causa de problemas financieros. Esto hace que la escena de los remailers sea muy dinámica. Cada cierto tiempo son desconectados determinados servidores y otros aparecen en su lugar. Private Idaho dispone de una función para actualizar automáticamente la lista de remailers. Con *Remailer/Update remailer info*, usted puede poner el programa al día siempre que quiera.

Bajo bandera falsa – falsificar el remitente del e-mail

En un mensaje anónimo el destinatario no ve el nombre de ningún remitente, o éste no le dice nada. Para él, en cierto modo, esto supone una ventaja. Al menos, sabe enseguida a qué atenerse con este e-mail. Pero también hay posibilidades para poner en un e-mail el nombre de un remitente concreto, aunque éste no tenga nada que ver con el mensaje. Hablando claro: se puede falsificar un mensaje, para que el destinatario atribuya la autoría a una determinada persona. Con lo que tomará su contenido en serio. Este procedimiento puede hacer mucho daño. Aunque técnicamente resulte mucho más sencilla, la falsificación de e-mail puede compararse con la de una carta real y puede traer consigo las correspondientes consecuencias por vía penal y civil. Razón por la que es mejor abstenerse de falsificar mensajes – aunque sea de broma.

INFO

Golpes bajos en el mercado laboral

Hace algún tiempo yo mismo conocí entre mis amistades un caso de falsificación de e-mail con nefastas consecuencias. Un amigo mío se presentó a la prueba de selección para un trabajo. Tras una satisfactoria entrevista en la que extraoficialmente se le aseguró el puesto, quedó convencido de tener en el bolsillo el trabajo de sus sueños. De repente, algunos días después, recibió de vuelta su solicitud de empleo acompañada de una carta en la que la empresa expresaba su pesar. Cuando mi amigo se informó allí, supo que – supuestamente – él mismo había declarado en un e-mail no estar interesado en ese puesto, por haber recibido una oferta mejor. En realidad, el aspirante jamás había escrito ese e-mail. Se trataba de una falsificación. Pero el trabajo ya se lo habían dado a otro y la víctima sólo pudo interponer una denuncia contra un desconocido. Naturalmente, no le sirvió de nada.

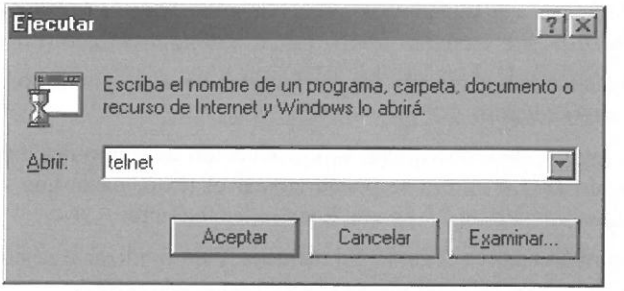
Falsificación de e-mail por Telnet

De buenas a primeras eso de falsificar un e-mail suena como algo muy laborioso, pero en realidad no es nada difícil. Ni siquiera se requiere un software especial. Basta con un simple programa Telnet, como los que van incluidos en el volumen de suministro de Windows. Con éste se puede hacer login en un servidor de correo saliente e imitar un programa de correo electrónico normal. Bastan unos pocos comandos para redactar así un e-mail y enviarlo.

Así de fácil es falsificar un e-mail

Cuando un programa de correo electrónico envía un mensaje al servidor de correo saliente emplea el *Simple Mail Transfer Protocol* SMTP. Este protocolo describe sólo unos pocos comandos, con los que se intercambian la cabecera y el mensaje. Estableciendo una conexión Telnet con el servidor de correo saliente cualquiera puede enviar esos comandos manualmente y, de este modo, crear un e-mail y enviarlo. Datos como, por ejemplo, el remitente, pueden ser confeccionados con total libertad y no dependen de los valores prefijados en el programa de correo electrónico. El siguiente ejemplo ilustra lo sencillo que es crear un e-mail falsificado. Con él sólo pretendemos mostrarle los grandes agujeros de seguridad del protocolo SMTP. Por favor, si hace la prueba, limítese a redactar mensajes dirigidos a usted mismo – una falsificación no deja de ser una falsificación.

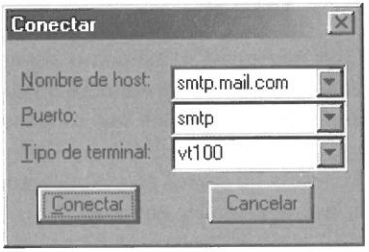
1. Primero hay que llamar al programa Telnet de Windows, seleccionando *Inicio/Ejecutar...* e introduciendo después el comando *telnet*.



A través del menú de ejecución, se puede llamar al programa Telnet de Windows.

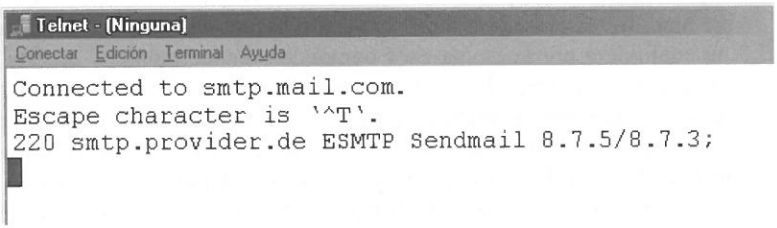
2. Ahora, seleccione la función de menú *Conectar/Sistema remoto...* para introducir la dirección del servidor de correo saliente.

3. Como nombre de host se emplea el del servidor, según viene indicado en la configuración del programa de correo electrónico. Como conexión, hay que introducir el puerto *smtp*.



Introduzca los datos de dirección del ordenador de salida del correo.

4. Al poco tiempo, el ordenador de correo saliente contestará con un breve mensaje de saludo. No hace falta registrarse. Ahora, podrá empezar a crear directamente el mensaje.



Ha sido establecida la conexión Telnet con el ordenador de salida del correo.

5. Primero el propio ordenador debe presentarse al ordenador correo saliente. Esto lo hace con el comando *HELO*.

6. A la confirmación le sigue ya el paso decisivo, es decir, la dirección del remitente. Ésta es transmitida con el comando *MAIL FROM:<dirección del remitente>*. Por ejemplo: *MAIL FROM:presidente@gobierno.es.*

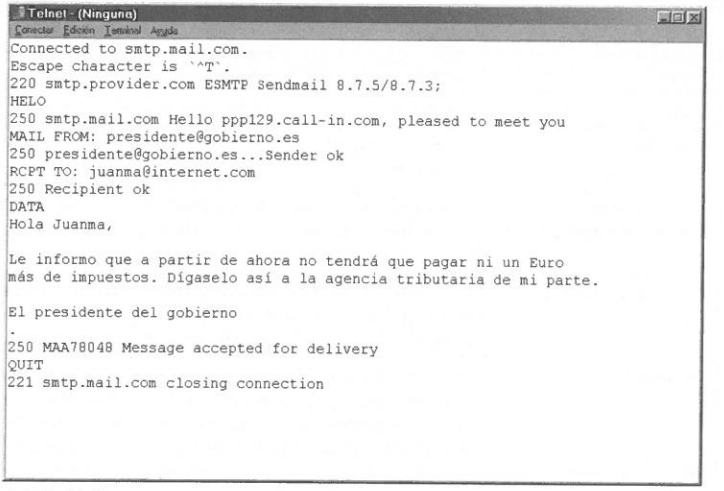
7. Después viene la dirección del destinatario con el comando *RCPT TO:juanma@internet.com.*

8. Acto seguido hay que iniciar la introducción del texto del mensaje con el comando *DATA*. Ahora se puede teclear el texto, hasta que se finalice la introducción con un "." en una línea independiente.

9. Esto también activa el envío del mensaje. Para finalizar la sesión con el servidor de correo saliente se introduce el comando *QUIT*.

Por suerte la mayoría de servidores de correo saliente ya han ido incorporando funciones de seguridad que impiden, o al menos dificultan, estos abusos. Actualmente cada vez hay más servidores SMTP que sólo reaccionan si se ha producido un inicio de sesión con identificador de usuario y contraseña. Sin embargo, todavía existen suficientes servidores de correo cuyas configuraciones son inseguras, ya sea por desconocimiento, pereza o ignorancia. Además, a los falsificadores recalcitrantes aún les queda la posibilidad de instalar su propio

servidor de correo y configurarlo según sus necesidades. Esto trae consigo unos gastos a cargo del propio bolsillo, pero quien quiera hacer daño a toda costa seguramente los asumirá.



Así de fácil es crear un e-mail con dirección falsa.

¿Podemos protegernos?

Si un amigo o compañero de trabajo ha descubierto en alguna dirección de Internet instrucciones para falsificar e-mail y quiere tomarle el pelo con eso, usted lo descubrirá en la mayoría de los casos. Si sospecha de un mensaje debería estudiar más a fondo su cabecera. Desgraciadamente, la mayoría de los programas de correo electrónico ocultan por norma esta información. Aunque, casi siempre, existe la posibilidad de echarle un vistazo a pesar de todo. En Outlook Express proceda del siguiente modo:

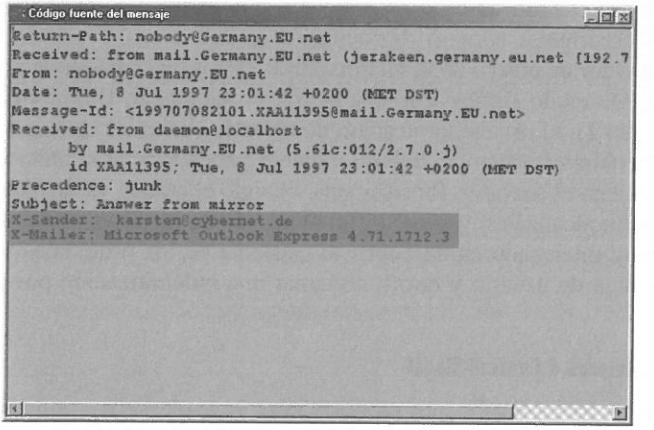
1. Abra el mensaje que quiera examinar más de cerca.
2. Seleccione la función *Archivo/Propiedades.*
3. Pase a la pestaña *Detalles.*
4. Aquí Outlook Express le mostrará tímidamente la información de cabecera como *Encabezados de Internet.*
5. Podrá ver más si hace clic sobre el botón *Cód. fuente del mensaje.* Ahora Outlook Express mostrará en formato bien legible todas las entradas de la cabecera. La siguiente tabla ilustra el significado de los datos de cabecera más importantes.

Nombre de la cabecera	Significado
From	La dirección de remitente que indicó el expedidor del mensaje. No tiene porqué coincidir con su dirección real.
To	La dirección de destinatario, que debería coincidir con la de usted.
Subject	La línea de asunto del mensaje.
Date	La fecha y la hora en que fue enviado el mensaje.
X-Mailer	El programa o sistema de correo que se utilizó para enviar el mensaje.
X-Sender oder X-Authenticated Sender	La dirección de remitente que anotó el servidor de correo del expedidor. Es mucho más fiable que la información From, ya que apenas puede ser manipulada.
X-Authenticated IP	Esta información es introducida sobre todo por los servicios de correo basados en la Red. Revela el número IP del ordenador desde el que fuera creado el mensaje.
Received	Todo servidor de correo que participara en el transporte del mensaje, deja su "matasellos" en forma de cabecera Received, depositando su propio nombre, el nombre del otro servidor implicado y la fecha de la transacción.

Todas las cabeceras que comienzan con una *X* son opcionales, es decir, pueden ir en un e-mail pero no son obligatorias. Aparte de la cabecera *X-Mailer* que figura en casi todos los mensajes, una cabecera con X siempre es una señal de aviso de que un mensaje no ha seguido del todo la ruta habitual.

6. Si un mensaje contiene una cabecera *X-Sender* compárela con la cabecera *From*. Si son diferentes, significará que el remitente ha indicado una dirección de correo electrónico distinta de la que usa realmente. Esto aún no tiene porqué significar nada raro, pero al menos revela al remitente verdadero.

7. Estudie, sobre todo, la cabecera *Received* con atención. Todo servidor de correo inscribe su marca al comienzo del mensaje. Es decir, la cabecera *Received* que figure abajo del todo será la del servidor de correo que haya empleado el remitente. Compare la dirección de este servidor de correo con la del remitente. Si los nombres del servidor son totalmente diferentes estaremos ante un nuevo aviso de que la dirección del remitente no es correcta. En este caso usted, al menos, conocerá el servidor de correo que utiliza esa dirección y podrá dirigirse al encargado correspondiente.



Las cabeceras X le revelan información sobre el verdadero remitente de un mensaje.

Desgraciadamente, una falsificación realizada con auténtica profesionalidad no puede ser descubierta de este modo. Aquí sólo nos queda el recurso de estar siempre en guardia ante la posibilidad de recibir una falsificación y, en caso de duda, preguntar al supuesto remitente si realmente redactó así su mensaje. Como alternativa, en áreas especialmente críticas de la comunicación existe la opción de trabajar por norma con sistemas de autentificación o encriptación. Estos dificultan considerablemente la falsificación de e-mail, o incluso la imposibilitan del todo. Un procedimiento de este tipo es PGP, que ilustraremos detalladamente más adelante en este mismo capítulo.

Bombas virtuales – paralizar sistemas mediante correo electrónico

El correo electrónico puede emplearse hasta como arma para bloquear un servidor de Internet, o incluso toda la red de una empresa. Basta con que la cantidad de mensajes enviados o su extensión sea lo suficientemente grande para que el objetivo del ataque caiga a nuestros pies. También es posible atacar con estas armas a usuarios comunes de Internet. En el presente apartado vamos a mostrarle cómo funcionan las bombas de e-mail y cómo nos podemos defender de ellas.

Así funcionan las cartas-bomba electrónicas

A veces, los medios más sencillos son los más eficaces. Una bomba de correo consiste en un número desmesurado de e-mail que se envía a la dirección de la víctima. Para aclararnos, no estamos hablando de centenares, sino de millares o más. Como alternativa, existe la posibilidad de emplear mensajes cuya extensión sea infinitamente mayor de lo normal, por ejemplo mediante archivos adjuntos.

No importa el contenido de cada mensaje. Lo que interesa es la cantidad y el tamaño. El descomunal número de mensajes recibidos casi simultáneamente colapsa al servidor de correo de la víctima, hasta llegar un momento en que éste se derrumbe. De modo similar a lo que ocurre en un ataque Denial-of-Service (vea el Capítulo 1), el ordenador acabará denegando cualquier otro servicio. El operador deberá invertir tiempo, trabajo y dinero para subsanar el daño y volver a poner en marcha el servidor. Precisamente cuando el ataque va dirigido a particulares a quien alcanza es, por supuesto, al proveedor de acceso de la víctima, que estará muy interesado en descubrir al causante de los problemas y podría retirar la licencia de usuario y quizá, reclamar una indemnización por daños y perjuicios.

INFO

La carta-bomba a Canter&Siegel

Una de las cartas-bomba más espectaculares ya explosionó a principios de los años 90. En aquel tiempo, el bufete americano de abogados Canter&Siegel intentó hacer clientes para la lotería anual de la "Greencard". Con ésta, el gobierno americano sortea cada año permisos de trabajo para extranjeros. Como entonces Internet ya había iniciado su gran boom, a los abogados se les ocurrió la idea de buscarse los clientes allí. Así que enviaron el correspondiente mensaje a todos los grupos de noticias existentes en aquella época. Este procedimiento indignó sobremanera a los lectores de estos grupos, que lanzaron una contraofensiva. En una reacción organizada, inundaron en pocas horas los servidores de correo de los abogados con decenas de miles de mensajes. El ordenador del proveedor de Internet no pudo hacer frente a este crecimiento y expiró. La acción no erró el blanco. El operador retiró la licencia de usuario a los abogados.

Más información sobre el asunto Canter&Siegel:
http://www.eff.org/Legal/Cases/Canter_Siegel/

Pero también se puede atacar con cartas-bomba a particulares. Si, por ejemplo, usted envía a alguien cada día 10 Mb en archivos adjuntos a e-mail, seguramente no le hará ninguna gracia, en primer lugar porque le llenará el buzón de correo, de modo que los mensajes que lleguen después serán rechazados, y aparte de esto, porque descargar semejante volumen de datos resulta muy gravoso cuando se hace mediante conexión telefónica de pago.

Otra posibilidad es el *List-Linking*, una técnica que consiste en apuntar a la víctima como abonado al máximo número posible de listas de mailing (más información sobre listas de mailing bajo la dirección http://www.lisde.de/e_home.shtml). Disponiendo del software adecuado, estas inscripciones masivas pueden ser ampliadas con unos pocos clics del mouse a un número de 50 a 100 listas de mailing. Si cada una de estas listas envía cada día uno o más mensajes a los abonados, el buzón de correo electrónico pronto se desbordará.

TRUCO

Bombas de correo: ¿el arma del hombre de a pie?

Con un esfuerzo comparativamente pequeño, las bombas de correo logran un efecto bastante poderoso e inmediato. A pesar de todo, recomendamos desistir de usarlas, ya que frecuentemente no sólo hacen blanco en la víctima, sino también en otros clientes del proveedor afectado y, sobre todo, a éste mismo. Y a un particular atacado selectivamente, a veces también se le pueden causar daños no sólo virtuales si, por ejemplo, no recibe mensajes importantes para su negocio o le surgen considerables gastos adicionales por conexiones. Esto puede traer consigo reclamaciones por daños y perjuicios y, en algunos casos, incluso querellas contra los causantes.

Repeler las cartas-bomba

Mientras un proveedor con servidor propio de correo entrante apenas puede defenderse de las cartas-bomba, el usuario particular sí que puede hacer algo para evitar que le rebose la bandeja de correo. Hay programas auxiliares especializados en combatir los correos masivos y las cartas-bomba. A diferencia de un programa de correo electrónico normal, éstos no necesitan descargar los mensajes del servidor de correo entrante para analizarlas. *Email Remover*, por ejemplo, inicialmente sólo muestra una lista de los encabezados de mensajes disponibles. Si usted tiene dudas, aún puede solicitar una pequeña vista previa de los e-mail que figuren en la lista. De este modo, los mensajes no deseados pueden ser borrados inmediatamente del servidor de correo entrante. Sólo tras haber concluido esta acción, será cuando se inicie su programa de correo electrónico habitual para descargar los mensajes restantes y gratos.

TRUCO

Repeler los ataques por List-Linking

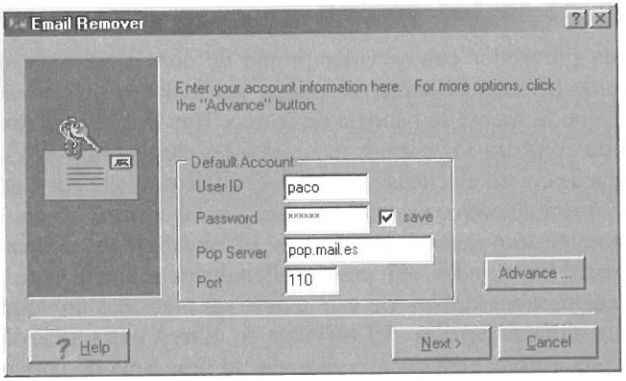
Un ataque por List-linking es muy difícil de combatir. En principio sólo hay dos posibilidades y ninguna de ellas es demasiado agradable. Una consiste en cancelar manualmente todos los abonos a listas de correo. Esto resulta muy engorroso y lleva tiempo, aunque es factible. Por otra parte, el malhechor podría repetir su acción en cualquier momento, con lo que habría que empezar de nuevo. La siguiente solución es algo más duradera: dé de baja su dirección de correo electrónico y solicite una nueva. Esto también supone algún esfuerzo, pero mientras el atacante no averigüe su nueva dirección, dejará de molestarle.

Email Remover – el tragaminas virtual

Email Remover es un programa gratuito, que puede ser descargado de http://eremover.bizhosting.com. En el primer arranque deberá configurarlo con la información de acceso al servidor de correo entrante, es decir, los datos que también emplee el programa estándar de correo electrónico que usted use.

1. Llame al Email Remover mediante el archivo ejecutable *Eremove.exe* y valide la primera ventana de saludo haciendo clic sobre *Next >*.

2. En el siguiente paso introduzca los datos de su acceso de correo electrónico. En *User ID* inserte su nombre de usuario. Si usted quiere que el programa trabaje siempre automáticamente sin necesidad de teclear una contraseña, introduzca en *Password* su palabra secreta de acceso y active la opción *save*. En el campo *Pop Server* anote el nombre del servidor de correo entrante. En caso de duda, podrá extraer todos estos datos de la configuración de su programa estándar de correo electrónico. Después, continúe con *Next >*.

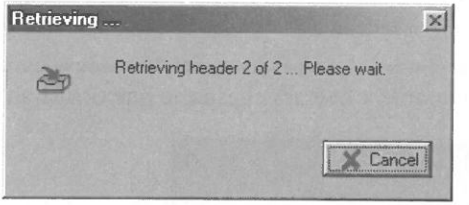


Anote aquí los mismos datos de acceso que tenga en su programa de correo electrónico.

3. Con esto habrá terminado la configuración necesaria y verá el menú de inicio, tal como será visualizado a partir de ahora cada vez que ponga en marcha el programa. Seleccione aquí la opción *I want to retrieve mail headers using below account.*

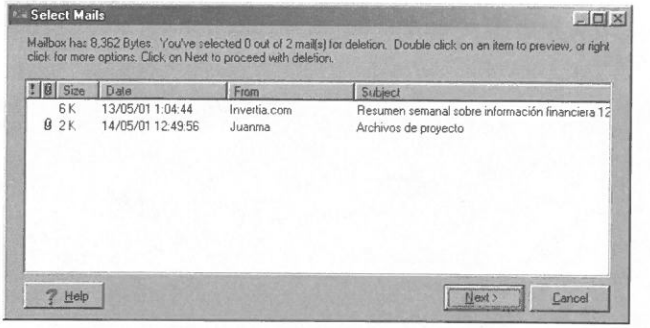
Desde el menú de inicio puede acceder a todas las funciones de Email Remover.

4. Ahora, Email Remover se registrará en el servidor de correo entrante y solicitará allí información sobre los mensajes disponibles. Sólo se transmitirán datos sobre los mensajes como el remitente, la línea de asunto y el tamaño, pero no los mensajes en sí. Usted puede seguir el proceso desde una ventana de estado.



Email Remover solicita información sobre los mensajes disponibles.

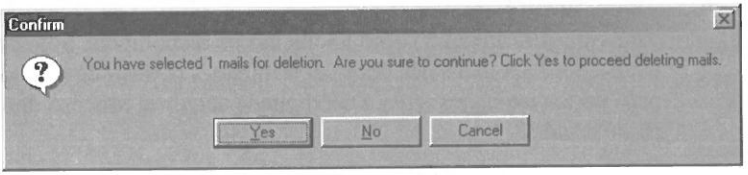
5. Acto seguido, Email Remover le presentará una lista de los mensajes disponibles. Para cada uno de ellos encontrará el tamaño, la fecha, el remitente y la línea de asunto. Si, en caso de duda, usted quiere saber algo más sobre algún mensaje en concreto, haciendo doble clic sobre su cabecera podrá solicitar una vista previa. En ese caso, el programa recopilará, además, las primeras líneas del mensaje y las visualizará en una ventana independiente.



El programa muestra la lista de mensajes disponibles.

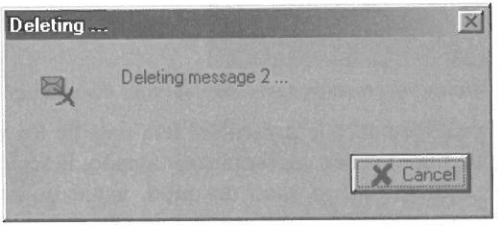
6. Si usted quiere borrar uno o varios mensajes del servidor de correo entrante, sitúe el mouse sobre él y márquelo con un solo clic (otro clic más volvería a quitar la marca). Una vez seleccionados todos los mensajes que desee borrar, haga clic sobre el botón *Next >*.

7. Antes de que Email Remover elimine definitivamente los mensajes seleccionados, tendrá lugar una confirmación de seguridad para prevenir borrados accidentales. El programa volverá a resumir el número de mensajes a borrar. Si usted quiere seguir adelante con el borrado, confírmelo con un clic sobre *Yes*.



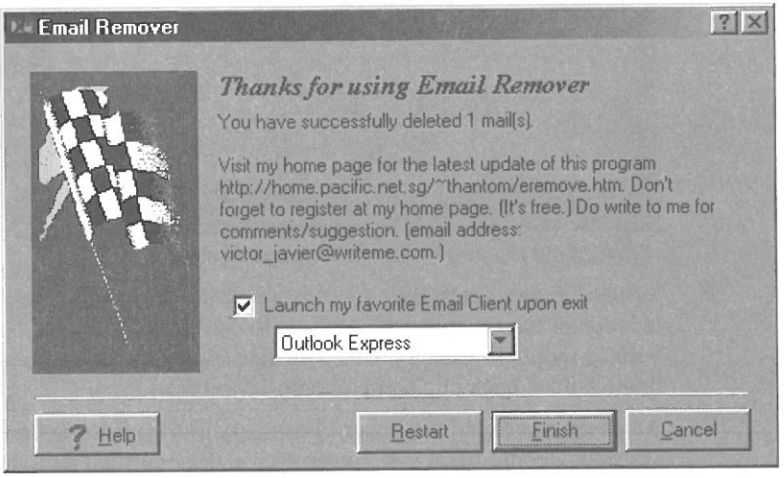
Confirme con Yes la consulta de confirmación previa al borrado de los mensajes.

8. Ahora, el programa eliminará definitivamente los mensajes marcados del servidor de correo entrante y liberará el espacio que ocuparan.



Email Remover borra del servidor de correo entrante los mensajes no deseados.

9. Para finalizar, el programa le ofrecerá arrancar automáticamente su aplicación estándar de correo electrónico para leer los e-mail que hayan quedado. Active para ello la opción *Launch my favorite E-Mail-Client upon exit* y elija en la lista su programa de correo electrónico, antes de hacer clic sobre *Finish*.



Para finalizar, Email Remover puede arrancar automáticamente su programa de correo electrónico.

Virus de e-mail, ¡no, gracias! – la configuración del programa de correo electrónico

En el pasado más reciente levantaron gran revuelo ciertos virus de e-mail, como el tristemente célebre "I love you " y sus afines. Hasta entonces se suponía que los virus sólo podían ser transmitidos por e-mail a través de archivos binarios. Sin embargo, hackers ingeniosos encontraron agujeros de seguridad, a través de los cuales se pueden introducir virus también en e-mail HTML. Aprovechan el hecho de que, al recibir e-mail HTML, el programa de correo electrónico se comporta igual que un navegador web y ejecuta componentes activos del código HTML. Así, es posible emplazar en un e-mail scripts capaces de ejecutar casi cualquier función en el PC del destinatario.

INFO

Peligrosa declaración de amor: "I love you" infecta Internet

En mayo de 2000, el virus de e-mail "I love you" consiguió propagarse a escala mundial por todo Internet, en cuestión de pocas horas. Además causó una histeria en los medios de comunicación, como tal vez no se había vivido jamás en relación con Internet. ¿Qué había ocurrido? Un hacker filipino de la nueva generación había creado un script en el lenguaje de macros de *Microsoft Visual Basic Script (VBS)* y lo había enviado con el texto "I love you" ("Te quiero") en la línea de asunto. Debió suponer, no sin razón, que a todo el mundo le gusta abrir un mensaje así. Si el e-mail era abierto con un programa de correo electrónico de Microsoft, el script accedía a los datos de la agenda de direcciones y reenviaba el mensaje a todos los destinatarios que figurasen en la misma. Esto hizo que el virus se expandiera con la rapidez de una avalancha. De paso, el script también atacaba datos multimedia como, por ejemplo, archivos MP3, dejándolos inservibles.

Debía ser un hacker de gran talento, pensará usted ahora. Pues no. El script no es nada espectacular. Simplemente saca partido del hecho de que todos los programas de correo electrónico de Microsoft soportan VBS y ejecutan sus extensiones correspondientes automáticamente. El propio acceso a la agenda de direcciones, el envío de más mensajes y la manipulación de archivos, son funciones que VBS facilita sin ningún tipo de trucos.

Más información sobre el virus "I love you":
http://www.zdnet.com/zdnn/special/lovebites.html

Así funcionan los virus de correo

Los e-mail pueden ser peligrosos si contienen archivos adjuntos. Como existe la posibilidad de adjuntar a un e-mail cualquier archivo, este anexo también puede ser un archivo ejecutable. Ni siquiera hace falta que sea un archivo EXE. Puede tratarse de cualquier archivo script. Los scripts no son archivos binarios, sino que contienen un texto que consta de instrucciones en determinado lenguaje script. Si el ordenador del destinatario posee un programa interpretador capaz de

comprender y obedecer a estos lenguajes script, al activar el archivo adjunto se ejecutará el script.

Actualmente, gracias a que Internet depende de los scripts para poder ofrecer páginas web interactivas y dinámicas, existen varios lenguajes script disponibles. Los más extendidos son *JavaScript* y *Visual Basic Script*. Este último lenguaje de Microsoft es especialmente peligroso. Como ya indica su nombre, está estrechamente emparentado con la familia Visual Basic, también de Microsoft. Aparte del lenguaje script VBS, esta familia la componen igualmente el lenguaje de programación *Visual Basic* y el de macros *Visual Basic for Applications* (VBA), con el que trabajan las aplicaciones Office de Microsoft. Este estrecho parentesco ha resultado ser funesto, ya que todos los miembros de las familias Visual Basic emplean el mismo modelo objeto. Así, un script VBS puede acceder sin mayores problemas a los datos y las funciones de una aplicación Office instalada en el ordenador. Ésta, a su vez, no está sujeta prácticamente a ninguna restricción de seguridad en lo que respecta al acceso a archivos y datos locales.

Justamente este hecho es el que aprovechó el creador del virus "I love you". Se limitó a escribir un script VBS, que verificaba si el PC del destinatario tenía una agenda de direcciones Windows. Si la encontraba, leía todas las direcciones de correo electrónico que contuviera y hacía que el programa de correo electrónico enviara, por su cuenta, una copia suya a todos esos destinatarios. Para eso no hacían falta trucos especiales ni conocimientos de experto. Todas las funciones de VB para el control remoto de la agenda y del programa de correo electrónico son conocidas y han sido bien documentadas por Microsoft. En este punto vamos a ahorrarnos la reproducción concreta del script. Primero, porque no queremos instigar a posibles imitadores y, segundo, porque con eso no haríamos otra cosa que impartir rudimentos de programación de scripts con VBS.

Para el éxito del virus "I love you" no fue decisiva precisamente una programación astuta, sino una serie de factores adicionales que aprovechó su diseñador (quizá ni siquiera de modo consciente):

- el estrecho entrelazamiento de los lenguajes de programación VB, que hemos descrito ya sobre estas líneas,
- la amplia difusión a escala mundial del software de Microsoft (este virus prácticamente afecta sólo a usuarios de productos Microsoft),
- la actitud relativamente descuidada de Microsoft y también de muchos usuarios en cuestiones de seguridad, así como
- el hecho de que la tecnología VBS sea instalada y activada de modo estándar en los PC con Windows, sin que los usuarios lo sepan y a pesar de que casi nadie usa realmente estas funciones.

Una curiosidad especial: según la interpretación de Microsoft, todo esto no son desventajas sino ventajas de los productos. En los últimos años, Microsoft ha ido incrementando cada vez más la interoperabilidad entre los productos y ha inte-

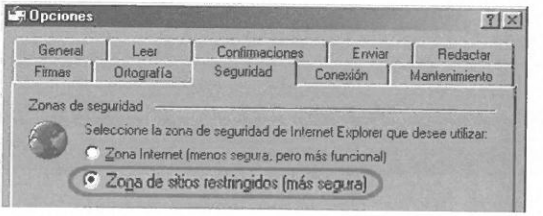
grado, además, extensas funciones de Internet. El virus "I love you" aprovecha de modo consecuente esta gran integración, demostrando así patéticamente lo potentes que son los productos de Microsoft y lo mucho que se descuidaron las cuestiones de seguridad durante su desarrollo.

¿Debemos renunciar por eso totalmente a los productos de Microsoft? Bueno, algunos lo hacen – por diversas razones – y es factible. En el mercado de software hay suficientes alternativas, que no tienen porqué ser de peor calidad ni más caras. Por otro lado, con la configuración adecuada podemos hacer que también los productos de Microsoft resulten seguros, de modo que los podamos emplear casi sin reservas. Aún nos quedaría el riesgo de los errores de programación y los agujeros de seguridad, pero esto también ocurre con otros productos.

Inmunizar Outlook Express contra los virus

Por desgracia, el popular programa de correo electrónico Outlook Express es uno de los más propensos a contraer virus. Su integración con Internet Explorer y el sistema operativo de Windows ofrece a los hackers una amplia gama de puntos de ataque. No obstante, también este programa puede ser protegido con la configuración adecuada.

1. Arranque Outlook Express y con *Herramientas/Opciones...* abra la configuración del programa.
2. Pase aquí a la pestaña *Seguridad*.
3. En el apartado *Zonas de seguridad*, usted controla la zona de seguridad que deberá emplear Outlook Express cuando maneje e-mail HTML. Esta configuración se basa en el concepto de seguridad de Internet Explorer, presentado exhaustivamente en el Capítulo 3.
4. Como configuración estándar Outlook Express emplea los valores de la *Zona Internet* para visualizar e-mail formateados con HTML. En estos casos, es más seguro si activa la configuración de *Zona de sitios restringidos*. Ésta suele ser mucho más restrictiva y no permite la ejecución de contenidos activos, como por ejemplo scripts.



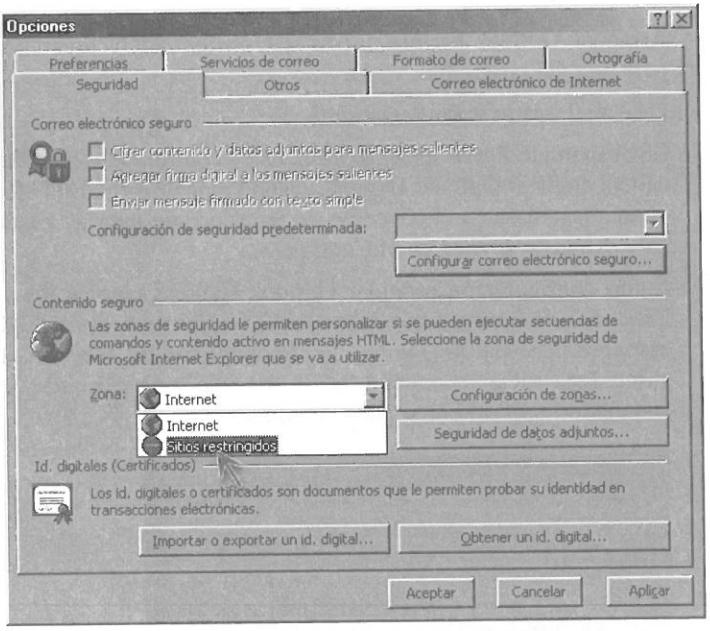
Por razones de seguridad, active para los e-mail la zona de sitios restringidos.

5. Guarde las nuevas configuraciones con *OK*.

Inmunizar MS Outlook contra los virus

También Outlook, módulo de Office, puede ser protegido con la configuración adecuada. El modo de proceder es el mismo que en Outlook Express, aunque hay pequeñas diferencias en los menús.

1. Arranque Outlook y, mediante *Herramientas/Opciones...*, se mostrará el cuadro de diálogo de configuración del programa.
2. Pase aquí a la pestaña *Seguridad*.
3. En el apartado *Contenido seguro* elija la zona de seguridad que deba emplear con Outlook cuando maneje e-mail HTML. Esta configuración se basa en el concepto de seguridad de Internet Explorer, presentado exhaustivamente en el Capítulo 3.
4. Por valor estándar Outlook emplea la configuración de la *Zona Internet* para visualizar un e-mail que contenga scripts o elementos HTML. En estos casos es más seguro activar la configuración de *Sitios restringidos*. Estas son, por norma, mucho más restrictivas y no permiten la ejecución de contenidos activos, como por ejemplo scripts.



También en Outlook, debería elegir la zona Sitios restringidos, que es más segura.

5. Guarde las modificaciones de configuración con *Aceptar*.

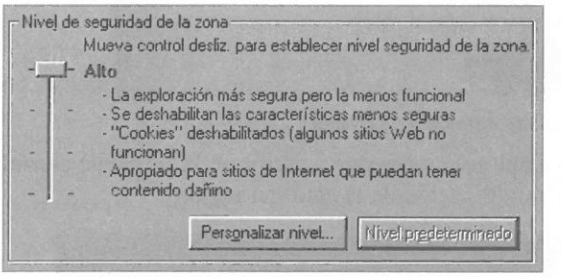
Verifique la configuración de la zona de seguridad

Para ir a lo seguro, le recomendamos que verifique si la configuración de la zona para sitios restringidos está bien ajustada para proporcionar a sus e-mail la máxima seguridad.

1. Arranque Internet Explorer y, desde *Herramientas/Opciones de Internet...*, acceda al cuadro de diálogo de configuración.
2. Pase ahora a la pestaña *Seguridad* y en el apartado de zonas seleccione *Sitios restringidos.*

Seleccione la zona de Sitios restringidos.

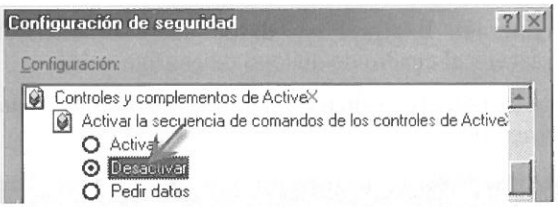
3. Verifique ahora en el apartado *Nivel de seguridad de la zona*, si para los sitios restringidos se ha especificado el nivel de seguridad máximo. De no ser así, desplace el cursor deslizante hacia arriba del todo, hasta que marque el nivel *Alto*.



Seleccione para los sitios restringidos el nivel de seguridad más alto.

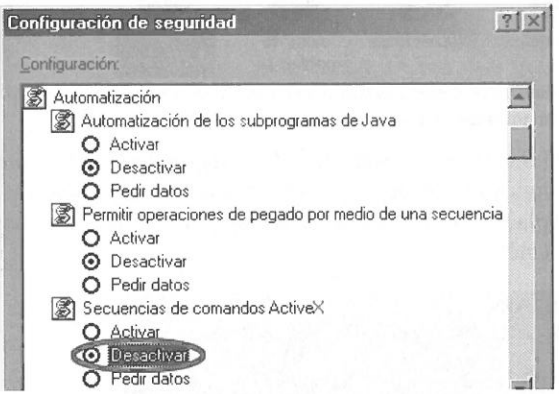
4. Por desgracia, hasta en el nivel de seguridad más alto Microsoft ha elegido dos configuraciones de seguridad de tal manera, que no ofrecen la seguridad máxima posible. Esto lo debería corregir usted manualmente, para lo que deberá hacer clic sobre *Personalizar nivel.*

5. En el detalle de configuración que aparezca, busque primero en el apartado *Controles y complementos ActiveX*. Aquí, ponga en *Desactivar* la primera opción *Activar la secuencia de comandos de los controles ActiveX marcados como seguros.*



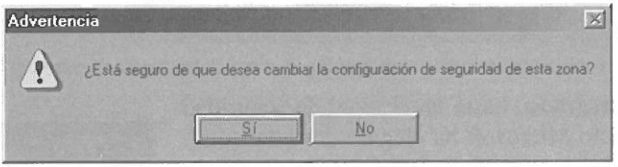
Desactive la ejecución de controles ActiveX...

6. Vaya avanzando en la configuración, hasta el apartado de *Automatización*. Cambie de nuevo a *Desactivar* la tercera opción, *secuencias de comandos ActiveX.*



...al igual que la ejecución de scripts.

7. Ahora, haga clic sobre *Aceptar* y confirme la siguiente consulta de seguridad para la modificación de la configuración.



Confirme con Sí la consulta de seguridad para la modificación de la configuración estándar.

8. Finalmente, haga un último clic sobre Aceptar para guardar la nueva configuración y volver a cerrar las opciones de Internet.

Con esto su programa de correo electrónico también estará protegido contra contenidos destructivos, cuando reciba y visualice e-mail con componentes dinámicos. Sin embargo, la función de protección también suprime elementos dinámicos e interactivos que no sean peligrosos, pero esto es algo que hay que aceptar en beneficio de una mayor seguridad.

El riesgo de HTML: e-mails formateados

Aparte de los archivos adjuntos virulentos hay otra fuente de infortunio en los e-mails: los mensajes formateados con elementos HTML. En realidad, un e-mail está compuesto de texto puro y sencillo. Pero como esto ya no cumplía las exigencias de la era multimedia, a la hora de redactar mensajes de correo electrónico también se quiso disponer de formatos como tipos y tamaños de tipografía, subrayados, colores, imágenes de fondo, etc. Precisamente las mismas posibilidades de las que se dispone para crear páginas web, por lo que parecía obvio aprovechar el formato HTML también para el correo electrónico. En resumen, un mensaje de e-mail formateado no es otra cosa que una página web enviada por correo electrónico. Una vez en el ordenador del destinatario, el programa de correo electrónico requiere al navegador, instalado de todos modos, que muestre el contenido del mensaje en condiciones ópticas.

Hasta aquí todo va bien, pero los e-mails formateados también heredan los riesgos de seguridad inherentes a las páginas web. Y es que una página web no sólo puede contener texto formateado, sino también instrucciones script que son ejecutadas automáticamente cuando la contemplamos. En consecuencia, lo mismo rige para los e-mails. Hay dos aspectos especialmente traidores:

- Muy pocos usuarios saben que un e-mail formateado con HTML puede ser tan peligroso como una página web. Por eso, con el correo electrónico no toman las mismas medidas de seguridad, ni mucho menos.
- Los programas de correo electrónico, como por ejemplo Outlook Express, disponen de una vista previa donde se visualizan automáticamente los mensajes nuevos, sin que el usuario deba hacer nada. Así, es muy posible que un e-mail que contenga un script llegue al ordenador y sea ejecutado automáticamente, sin un solo clic de mouse del usuario, cosa que impide aplicar incluso una regla de seguridad tan sencilla como "no abrir jamás e-mail de remitentes desconocidos".

TRUCO

Desactivar la función de vista previa en Outlook Express

La traidora función de vista previa puede ser desactivada en la mayoría de los casos. En Outlook Express, por ejemplo, hay que hacerlo con *Ver/Diseño* para mostrar el cuadro cuadro de diálogo y, desde allí, desactivar la opción *Mostrar panel de vista previa*.

Protección contra e-mails con elementos activos

La protección más eficaz contra e-mail activos es renunciar totalmente a usar formatos. Si nos ponemos de acuerdo al respecto con nuestros compañeros de correspondencia, al menos podremos abrir sin reservas los e-mail de los conocidos. Pero esto no sirve de nada si recibimos e-mail de otras personas. Aquí, hasta que no los abramos no podremos saber si contienen elementos activos o puro texto. En este caso, la alternativa más sencilla y segura sería usar un programa de correo electrónico, que ni siquiera disponga de un navegador web integrado y, por lo tanto, no pueda ejecutar los contenidos activos de los mensajes. Un producto recomendable de este tipo es Eudora (http://www.eudora.com). Entiende los formatos HTML sencillos, de modo que hasta nos permite ver en todo su esplendor los mensajes formateados. Pero ignora completamente contenidos activos como las instrucciones script, de modo que éstas no pueden causar ningún daño.

Sin embargo, también con Outlook o Outlook Express podemos recibir mensajes HTML, sin albergar reservas sobre su seguridad. La única condición es que hayamos especificado para los e-mail la zona de seguridad correcta, según lo descrito anteriormente, y la hayamos configurado adecuadamente. Así, también estos programas visualizarán sólo los propios formatos de HTML. Por el contrario, los elementos interactivos y dinámicos, como JavaScript o las instrucciones VBS, serán interceptados con fiabilidad por la configuración de seguridad.

Distinguir los avisos serios del alarmismo

En este punto queremos mencionar también un aspecto muy especial del tema correo electrónico y virus. Cada dos por tres, vagan por la red y los medios de comunicación avisos y noticias sobre supuestos virus de correo electrónico. Así, se dice que los e-mail en cuya línea de asunto figure "Good Times" o "Penpal Greetings", contienen virus destructivos que infectan al ordenador cuando se lee el mensaje, e incluso que pueden llegar a dañar el hardware. Naturalmente, las noticias sobre estos supuestos virus de e-mail son difundidas por correo electrónico y pueden convertirse en auténticas plagas, ya que funcionan siguiendo un esquema muy sencillo pero con indudable éxito:

1. En las misivas de alarma se exhorta al receptor a que envíe el texto a todos sus conocidos.
2. La mayoría de usuarios cumplen ese requerimiento, sin darse cuenta de que el verdadero malhechor puede ser el aviso de virus.
3. Como cada destinatario lo envía al mayor número de direcciones posible, éste se multiplica con gran éxito.

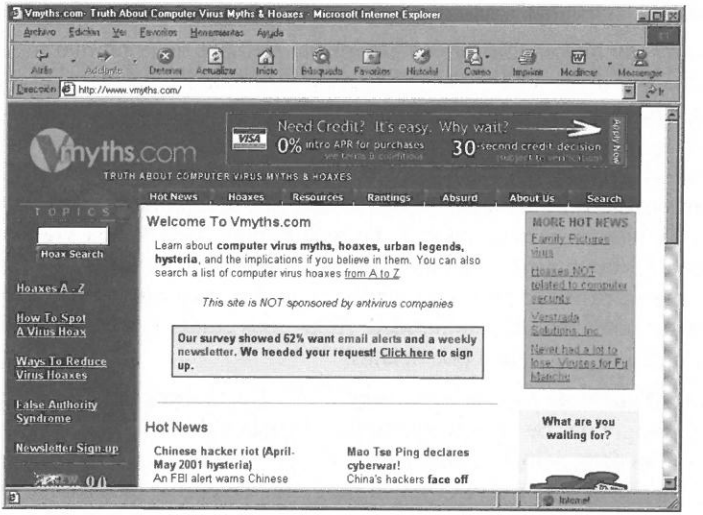
Por suerte, el cometido de estos virus es exclusivamente su propagación y no las acciones destructivas. Aunque por el mero hecho de difundirse estos avisos fal-

sos ya causan daños. La gran cantidad de e-mail que puede generarse por su culpa desperdicia inútilmente los preciosos recursos de transmisión de Internet. Para estos avisos falsos, que especulan con el desconocimiento o el miedo de los usuarios, se ha impuesto la expresión *Hoax*.

Reconocer un hoax de correo electrónico

Cuando reciba el aviso de un nuevo virus, ante todo no se deje llevar por el pánico.

1. Piense, en primer lugar, de qué fuente procede esa advertencia.
2. Un e-mail recibido inesperadamente – según lo descrito anteriormente – sin duda no es una advertencia seria.
3. También en las revistas de informática no demasiado serias, aparecen con regularidad falsos avisos de supuestos virus que desconciertan a los lectores.
4. Fíjese en la exactitud con que es descrito el supuesto virus. Si la descripción es muy general, puede que se trate de una broma o que el autor de la misiva no tenga mucha idea.
5. Los avisos de virus útiles dan referencias exactas sobre el comportamiento del virus y los síntomas para detectar una infección.
6. En caso de duda, ayuda visitar http://www.vmyths.com. Aquí encontrará una relación muy buena y siempre actualizada de los hoaxes sobre virus que circulan por ahí y, naturalmente, avisos sobre nuevas amenazas de virus que sí son reales.



En http://www.vmyths.com se informa sobre los "virus virtuales", es decir, hoaxes y alarmismo.

7.2 El correo electrónico como fuente de información – los riesgos de la correspondencia electrónica

Aunque los e-mail sólo se empleen regularmente para la comunicación, pueden suponer una amenaza. Sobre todo, si no se usan para enviar misivas nimias del tipo "Hola, ¿cómo estas?", sino para transmitir informaciones y datos importantes y confidenciales del entorno personal o de negocios. En este caso, existe el peligro de que el mensaje no sólo sea leído por el destinatario al que iba dirigido, sino también por otras personas que no tengan nada que ver. Observemos, de nuevo, cómo funciona el correo electrónico y repasemos sus posibles puntos débiles.

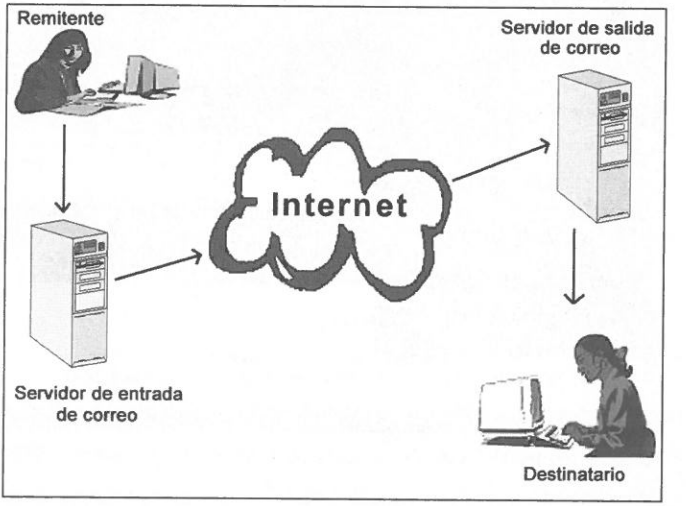
Postales electrónicas – por eso las puede leer cualquiera

Los e-mail son transmitidos mediante el *Simple Mail Transfer Protocol* SMTP, un protocolo algo entrado en años, pero muy sencillo y sólido. Aunque precisamente en su sencillez estriba el problema, ya que transmite los mensajes electrónicos en texto legible de ordenador a ordenador. Es decir, el texto que usted envía en un e-mail es transmitido tal cual a través de Internet. Por desgracia, carece completamente de un sobre electrónico que lo proteja. En realidad, en lugar de hablar de "carta electrónica", deberíamos emplear más bien la expresión "postal electrónica".

A esto hay que añadir que un e-mail no siempre tiene porqué tomar el camino más corto desde el PC de usted hasta el ordenador del destinatario. Más bien suele pasar por diversas estaciones intermedias hasta alcanzar la meta. En cada una de estas estaciones es guardado, al menos durante un breve tiempo, en una memoria intermedia hasta que sea transmitido al siguiente punto. Con eso, a un administrador de sistema curioso le sobraría tiempo para echar un vistazo rápido. Si, además, a alguien se le ha metido entre ceja y ceja vigilar sistemáticamente las comunicaciones que usted haga por correo electrónico, podrá "grabar" en una de las estaciones intermedias todos los mensajes que le interesen y analizarlos con absoluta tranquilidad. Aclaremos cuáles (y sobre todo, cuántos) son los objetivos de ataque potenciales:

1. El punto de partida es *su propio PC*, donde usted crea el mensaje. Muchos programas de correo electrónico disponen de funciones de registro o guardan para siempre jamás copias de los mensajes redactados. Todo aquél que tenga acceso a su PC y a su programa de correo electrónico podrá leer los mensajes que usted escribiera y recibiera.

2. El *servidor de correo saliente* de su proveedor de Internet. Aquí comienza el viaje de su e-mail a través de Internet. Si alguien quiere vigilarle selectivamente, esta sería la primera dirección a la que acudiría. ¿Que su proveedor jamás permitiría algo así? ¡Quizá sea precisamente él quien espía a sus clientes! Además, también existe la posibilidad de una orden de registro (para autoridades estatales, si hay una sospecha fundada), sobornos, o medidas de espionaje que el proveedor desconozca.
3. Desde el servidor de correo saliente de su proveedor, el viaje continúa. El destino es ahora el servidor de correo entrante del proveedor del destinatario. Pero hasta llegar allí el camino puede ser muy largo, ya que conduce a través de *numerosas máquinas de Internet*, que constituyen la conexión directa en Internet entre los dos ordenadores. El e-mail es transmitido en forma de paquetes de datos, cosa que dificulta su lectura, pero no la imposibilita.
4. Una vez alcanzado su destino, los paquetes de datos son convertidos de nuevo en un e-mail de texto legible en el servidor de correo entrante del proveedor de Internet del destinatario, donde será almacenado hasta que éste descargue su correspondencia. De nuevo, el *servidor de correo entrante* es la primera dirección a la que acudirán los espías que pretendan vigilar al destinatario.
5. En algún momento los mensajes son descargados y aterrizan en el *ordenador del destinatario.* Allí son almacenados de nuevo y conservados hasta que el receptor los borre. Naturalmente, también aquí existe la posibilidad de que el ordenador caiga en malas manos y una persona no autorizada lea los mensajes.



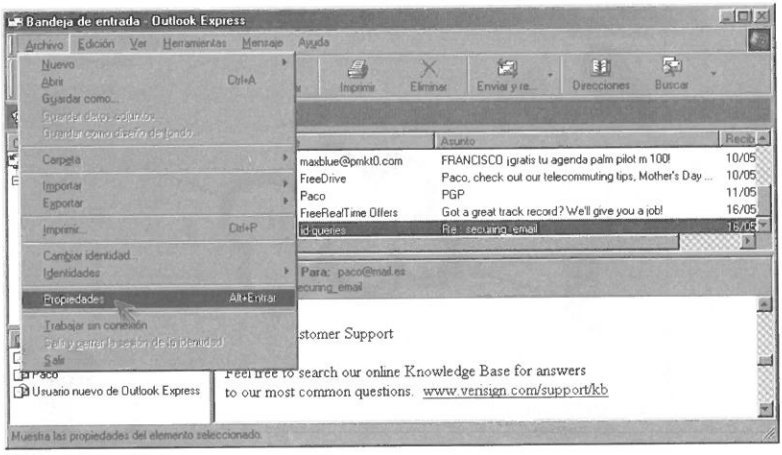
El recorrido de un e-mail desde el remitente hasta el destinatario, conduce a través de varias estaciones intermedias atacables.

Por consiguiente, la cadena de ordenadores que participan en el transporte de un e-mail no es precisamente corta. Incluso llega a alargarse, si se emplean direcciones de correo electrónico con redireccionamiento, apartados de correo electrónico colectivos o funciones de confort parecidas.

Seguir la ruta de un e-mail

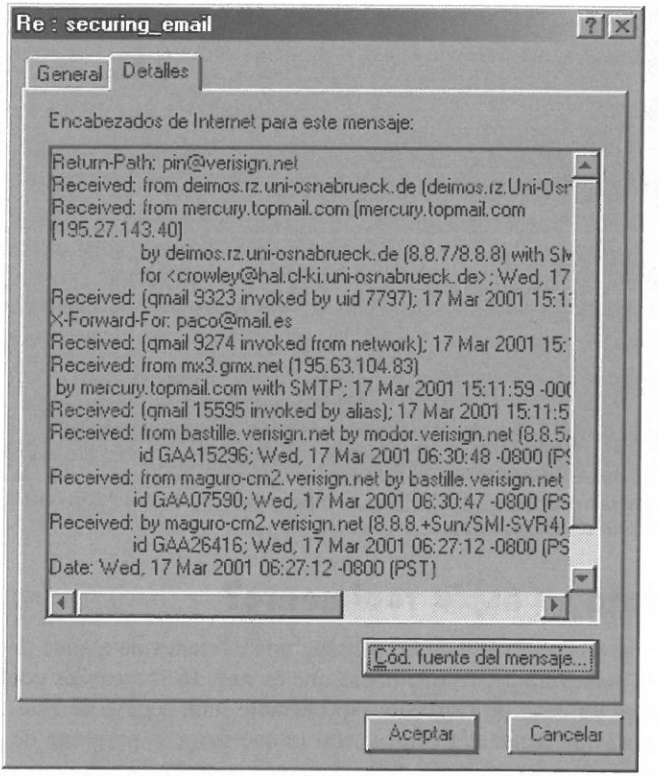
Si usted quiere convencerse por sí mismo de la ruta que ha tomado un e-mail desde el remitente hasta llegar a usted, podrá seguirlo en el header del e-mail. Se llama así a la cabecera, que contiene todos los datos importantes para el transporte del mensaje. En ésta, cada ordenador que participe en el transporte del mensaje añade una entrada con la fecha y hora. Este matasellos virtual permite seguir con exactitud el recorrido de un e-mail. Aunque las entradas Received sólo aparecen si usted solicita que el mensaje sea visualizado en texto fuente. Esto es algo que muchos programas de correo electrónico no hacen por norma, porque consideran que esta información no es relevante (cosa que en muchos casos es cierta). Las siguientes instrucciones describen a modo de ejemplo, cómo visualizar las entradas Received en Outlook Express.

1. Marque en la lista el mensaje que quiera examinar, o visualice ese mensaje directamente con doble clic.
2. Seleccione ahora la función de menú *Archivo/Propiedades*, para ver las propiedades del mensaje. (También dispone de una alternativa más rápida con [Alt] + [Entrar]).



Abra las propiedades de un mensaje para visualizar el código del mensaje.

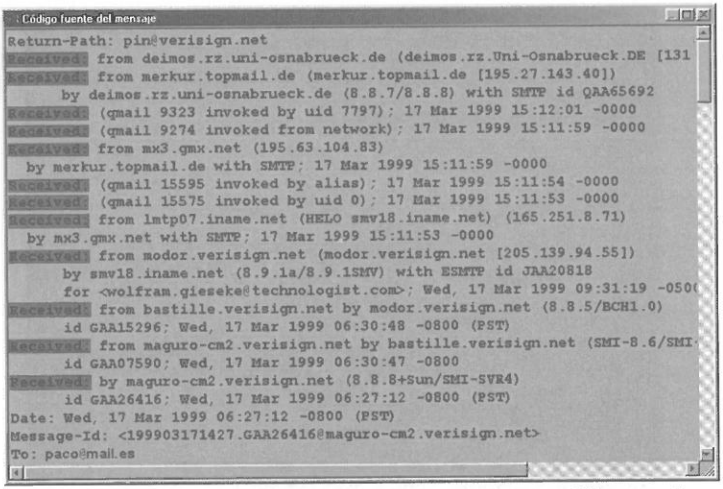
3. En el menú pase a la pestaña *Detalles*, donde aparecerá la cabecera en el apartado *Encabezados de Internet para este mensaje.*



En Propiedades-Detalles aparece toda la cabecera con sus entradas Received.

4. Aún lo verá más claro si, haciendo clic sobre *Cód. fuente del mensaje...* abre todo el mensaje en texto fuente. Ahora, aparecerá el texto en un editor de textos, donde lo podrá leer mejor.

5. Aquí encontrará en el margen superior las entradas *Received*. Deben ser leídas de abajo hacia arriba, es decir, la entrada más antigua del primer ordenador está abajo del todo. El sello Received que está más arriba suele ser el del servidor de correo entrante local. No se deje desconcertar por la información horaria que aparece en las entradas Received. Como Internet es universal pasa por numerosas franjas horarias, por lo que el tiempo indicado siempre es algo relativo.



Este mensaje pasó en total por 12 ordenadores de Internet diferentes, hasta que lo recibió el destinatario.

¿Cuánto se espía realmente?

Cuando se es consciente de las muchas posibilidades de ataque de que dispone un espía perseverante, resulta obvio que es muy fácil crear las condiciones técnicas para un caso de fisgoneo. No obstante, una acción de este tipo requiere cierto grado de recursos técnicos, con lo que surge la pregunta de si alguien se toma realmente esa molestia. Sólo podemos contestarla con matices.

Espionaje de usuarios particulares

Para los usuarios puramente particulares, que sólo intercambien por correo electrónico mensajes "inofensivos", el peligro no es demasiado grande. Mientras sus misivas sean de carácter meramente personal, por regla general no se puede sacar provecho de ellas. Así que, no vale la pena espiarlas. Aquí, el único peligro podría provenir de chiflados, o de conocidos que quieran vengarse – ¿quizá un(a) ex despachado(a), o algo así?. Y el correo electrónico también puede ser una excelente fuente de información, si un hacker quiere espiar a una persona concreta.

La cosa cambia si un particular desempeña actividades que atraigan el interés de determinados círculos. Si alguien, por ejemplo, está próximo a grupos políticos radicales, puede caer rápidamente en el campo de mira de la brigada de interior. No es que a ésta se le permita automáticamente todo, pero sí que posee las posibilidades técnicas y los permisos. Aunque en un estado constitucional, para eso se requiere una orden judicial (comparable a una orden de registro).

Espiar a usuarios comerciales/profesionales

Cuando hablamos del correo electrónico en el ámbito de los negocios, entramos inevitablemente en el tema del espionaje económico. Éste es un ramo increíblemente floreciente, donde no se escatiman dinero ni esfuerzo para hacerse con la información de la competencia. Si alguien envía por correo electrónico las actas de reuniones confidenciales y proyectos, corre el riesgo de que terceros no autorizados también lean esta información. Por cierto, esto también ocurre cuando los correos sólo son distribuidos dentro del intranet de la empresa, ya que éste también ofrece posibilidades técnicas para el espionaje.

Quien tramite directamente negocios por correo electrónico, como por ejemplo la concesión de pedidos, debería protegerse sin falta. El correo electrónico no sólo es peligroso porque alguien pueda leer el contenido. Los mensajes electrónicos no son precisamente inmunes a las falsificaciones, de modo que unos pedidos manipulados o falsos pueden causar problemas terribles (lea al respecto el primer apartado de este capítulo).

¿Estado policial? – extensa vigilancia del correo electrónico

Constantemente surgen rumores de que la NSA (*National Security Agency*, Agencia Nacional de Seguridad de los Estados Unidos) o también el *Bundesnachrichtendienst BND* (el Servicio Secreto Federal de Alemania) intercepta sistemáticamente la comunicación por correo electrónico en todo el mundo. Cuando los rumores se mantienen con tanta tenacidad, casi siempre hay algo de verdad. Pero, ¿cómo se supone que es esa vigilancia? Cada día circulan millones de correos electrónicos por Internet. Cada uno sigue su propio camino hasta llegar al destinatario. Aunque, sin duda, habrá algunos ojos de aguja por los que deban pasar muchos e-mail, como por ejemplo las líneas transatlánticas desde Europa hasta los Estados Unidos.

En principio resulta factible la idea de instalar puestos de vigilancia en estos nodos. Eso permitiría registrar una parte relativamente grande de la comunicación por correo electrónico en todo el mundo. Pero, ¿qué se podría hacer con los datos registrados? Su cantidad sería tal que, por grande que fuera la plantilla de empleados dedicados a leerlos, no podrían hacer frente a todos. Por lo tanto, lo único factible sería analizar esos datos mecánicamente. Los ordenadores podrían explorar los textos en busca de determinadas palabras clave, como por ejemplo "armas", "drogas" o "uranio", por mencionar algunos ejemplos cercanos. Además, existiría la posibilidad de registrar automáticamente todos los mensajes enviados o recibidos por una persona concreta.

Por consiguiente, técnicamente una vigilancia extensa sería factible e imaginable. Quizá ya exista tal como la hemos descrito, o de otro modo. Aunque tam-

bién en este caso se puede decir que, si uno se mantiene alejado de temas sospechosos, no tiene motivo de preocupación. El ligue pasajero del último fin de semana quizá interese a la esposa, pero no a la brigada de interior.

INFO

Carnivore – El FBI también escucha

Hace ya algún tiempo el FBI desarrolló un programa con el significativo nombre de *Carnivore* (en español, carnívoro). En este caso la expresión programa no sólo hace referencia al software, sino también a un modo de proceder y a las bases legales necesarias para vigilar el tráfico de e-mail de personas concretas. El FBI instala en el equipo del proveedor de la víctima a la que quiera espiar un software que copia para sus agentes todos los mensajes que sean relevantes. Oficialmente este procedimiento sólo puede ser empleado para la investigación y persecución cuando hay un indicio justificado de criminalidad. Pero resulta difícil imaginar que un instrumento tan poderoso no sea empleado también para otros fines. Hasta la fecha, Carnivore sólo existe en los Estados Unidos. Aunque quizá no sea más que cuestión de tiempo, que también en este país la policía y los servicios secretos impongan una solución de este tipo.

Más información sobre Carnivore:
http://www.stopcarnivore.org/
http://www.robertgraham.com/pubs/carnivore-faq.html

Quizá el peligro mayor para la confidencialidad de nuestros e-mail no parta del BND ni de la CIA, sino de los administradores del sistema. Éstos, a veces, simplemente se aburren o no tienen ganas de trabajar "de verdad", por lo que les gusta revolver en los archivos de correo de sus usuarios. A fin de cuentas, técnicamente es muy fácil y un administrador de sistemas experto, tampoco deja huellas. Con esto no queremos desacreditar a todo un colectivo profesional, pero, por desgracia, siempre hay alguna oveja negra y ya han salido a la luz algunos casos de este tipo. Se dice que el siniestro porcentaje aún es bastante más alto. Es decir, lo que usted jamás contaría a su administrador de sistema ante una taza de café, tampoco lo debería mencionar en un e-mail desprotegido. Especialmente los asuntos personales, si es que está permitido resolverlos por el correo electrónico de la empresa, pueden convertirse rápidamente en un arma arrojadiza en manos de alguien aficionado al mobbing (vea al respecto el Capítulo 6).

TRUCO

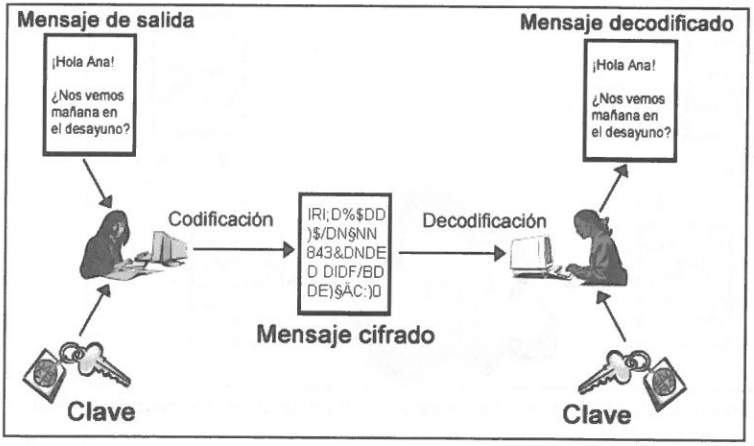
¿En qué se nota que el e-mail ha sido leído por alguien?

¡Ojalá fuera tan sencillo! Al recibir un mensaje parpadea una bombillita roja y una voz amable advierte, que ese correo ya ha sido abierto una vez. Por desgracia, la cosa no funciona así. Los espías del correo que se limitan a leer los mensajes no dejan ni una sola huella. Por eso, la única posibilidad de proteger la confidencialidad de los e-mail consiste en tomar medidas preventivas. Sólo si usted ya tiene una sospecha concreta la podrá comprobar. Deslice en sus e-mail información intencionadamente falsa como cebo y espere, a ver si alguien intenta sacar partido de ella.

Contramedidas: encriptar los mensajes

Como el e-mail no es más que una especie de postal electrónica, sólo hay una posibilidad de hacerlo más confidencial. Ésta consiste precisamente en proporcionarle un sobre electrónico. La finalidad de este sobre es la misma que tiene en una carta de verdad: proteger el mensaje de los lectores entrometidos mientras el e-mail esté en camino. Pero en contraste con un sobre de verdad, la envoltura electrónica hace algo más, ya que ha sido concebida para que sólo la puedan abrir determinadas personas autorizadas.

Para proteger un e-mail con un sobre virtual de este tipo se puede emplear una encriptación. Ésta lo que hace es aplicar determinado procedimiento matemático para convertir el contenido original de un mensaje en un barullo de caracteres aparentemente aleatorio. Estos caracteres inexpresivos pueden ser enviados sin problemas a través de Internet. El destinatario empleará el mismo procedimiento matemático a la inversa, para reconstruir el texto original a partir de la misiva encriptada. Para que ese mensaje no pueda ser descodificado por cualquiera que conozca y domine ese procedimiento matemático, remitente y destinatario usan, además, una clave privada que decide la valoración exacta de los caracteres.



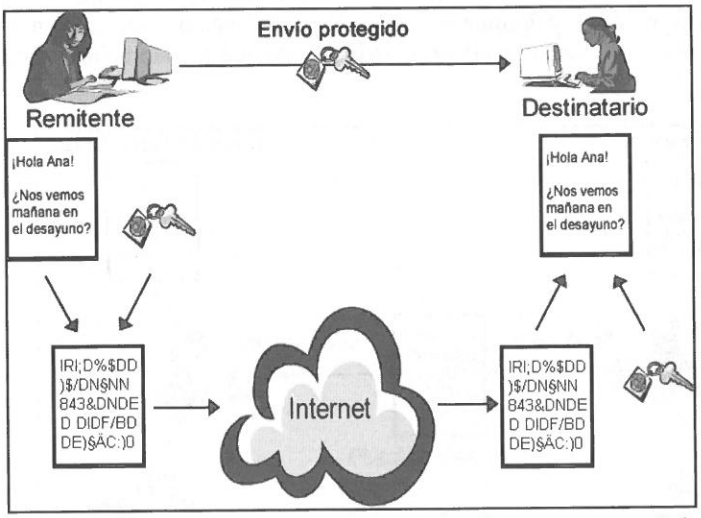
Así funciona la encriptación de mensajes.

Encriptación simétrica

En la variante más sencilla de encriptación, el remitente y el destinatario emplean la misma clave (simétrica). El gran problema de la encriptación simétrica es que las dos partes de la comunicación deben intercambiarse la clave antes del primer envío de mensajes. Lógicamente, al no disponer aún de la clave común,

este acuerdo debe establecerse sin codificación. Para efectuar el intercambio, en ningún caso deberá emplearse la misma ruta por la que se vayan a enviar más adelante los mensajes. Eso equivaldría a dar, literalmente, las llaves de la propia seguridad a aquellos contra cuya vigilancia debía proteger la encriptación.

Por consiguiente, las claves simétricas siempre deben ser intercambiadas por los usuarios utilizando la vía más segura. Según cuál sea el procedimiento de encriptación, esto quizá pueda hacerse por teléfono. Pero para claves digitales complejas se necesitan disquetes o soportes de datos similares. Como la seguridad desaconseja enviar estos soportes por correo convencional, un encuentro personal sería el método más indicado y más seguro. Pero, ¿y si la otra parte no vive en el mismo continente? ... Como habrá podido ver, hasta que se pueda iniciar el intercambio de mensajes con claves simétricas se requiere algo de esfuerzo. Aunque esto no significa que esta técnica no sea segura y aplicable. Siempre que se encuentre la posibilidad de enviar la clave por un camino seguro este procedimiento es, con mucho, el más eficaz.



El problema de la encriptación simétrica está en la entrega segura de la clave.

DES – Data Encryption Standard

Puede que el representante más conocido del procedimiento de encriptación simétrica sea ***Data Encryption Standard***. Fue desarrollado ya a comienzos de los años setenta por IBM y la NSA (National Security Agency, un servicio secreto de los Estados Unidos). El hecho de que hoy en día siga de actualidad, ya dice mucho sobre su seguridad.

DES subdivide los datos a encriptar en bloques de 64 Bits de tamaño. Los datos contenidos en esos bloques son modificados al encriptarse en 16 pasadas. Para hacer esto sólo dispone de tres posibilidades de manipulación:

- en el *vínculo de O-exclusiva*, a partir de dos secuencias de bits se crea una nueva,
- en la *sustitución*, una secuencia de bits es sustituida por otra y
- en la *permutación* el cambio tiene lugar dentro de una secuencia de bits.

En este proceso una clave, cuyo tamaño también es de 64 bits, controla qué operaciones se ejecutan y por qué orden. Los datos sólo podrán ser desencriptados posteriormente con esa clave para lo cual, en principio, se ejecuta todo el proceso a la inversa.

INFO

¿Hasta qué punto es seguro DES?

La seguridad de DES es relativa. Su modo de funcionamiento hace que una clave sólo pueda ser descifrada a la fuerza, es decir, probando todas las variantes posibles. Desgraciadamente, ya cuando este método fue desarrollado, la NSA implicada limitó por razones políticas la longitud de la clave a 64 bits. Esto facilita los ataques que impliquen muchos cálculos. Hasta la fecha sólo se ha conocido un ataque a DES que haya tenido éxito. Aunque no existe la menor duda de que, si lo necesitan, los servicios secretos y el ejército pueden reventar la clave DES. Pero en la frecuente aplicación de DES para claves de sesión temporales, se puede pasar por alto este peligro.

Hoy en día, DES es utilizado por muchos sistemas en el entorno de Internet y On-line. Por ejemplo, lo emplean los fiables protocolos de WEB que son *S-HTTP* y *SSL*, al igual que el estándar de Homebanking HBCI. Para compensar la debilidad de su clave excesivamente corta, fueron desarrollados diversos procedimientos a imagen y semejanza de DES. Entre los más conocidos está el *International Data Encryption Algorithm* (IDEA). Una variante directa de DES es *Triple-DES*. Aquí, la encriptación consiste en tres ejecuciones sencillas de DES, de las cuales la mediana es técnicamente una descodificación. Como cada ejecución emplea su propia clave, resulta una longitud de clave total de hasta 192 bits. Con claves de esta longitud resulta prácticamente imposible probar todas las variantes.

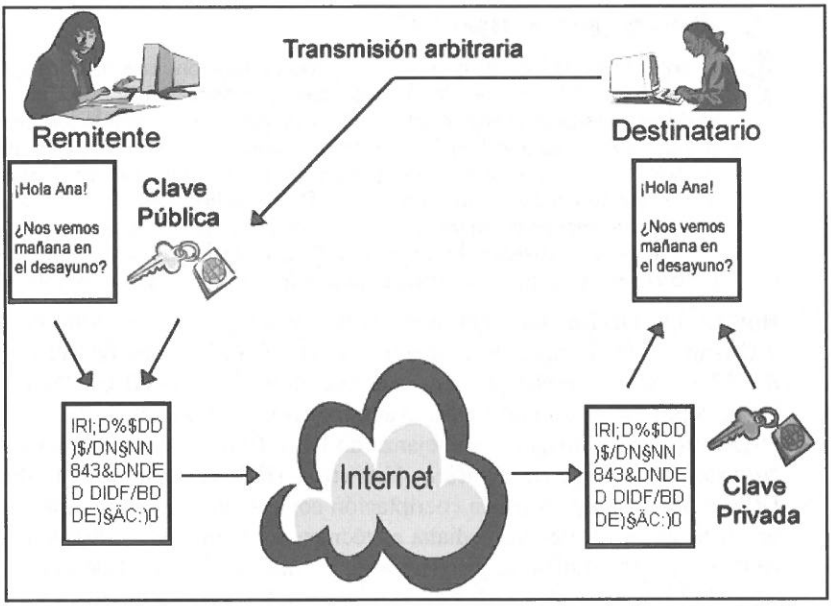
Claves asimétricas

Para resolver el problema de la entrega de claves se desarrollaron las claves desiguales (asimétricas). En este caso, en lugar de una clave individual cada usuario posee una pareja de claves propia.

- Una *clave privada* sólo va destinada al propietario y debe permanecer en secreto a toda costa. Esta clave puede encriptar mensajes y transformar de nuevo en legibles a los que fueran codificados con la clave pública.

- Una *clave pública* va destinada a ser repartida entre los compañeros de comunicados del propietario de la clave. Se emplea para enviar mensajes al propietario, que sólo él podrá convertir en legibles con su clave privada. A la inversa, usando la clave pública se puede comprobar la firma de un mensaje rubricado con la clave privada. Esto permite verificar la autenticidad de un mensaje.

Por consiguiente, cada una de las dos claves descifra los mensajes que fueran encriptados previamente con la otra clave. A pesar de todo, la clave pública no permite sacar conclusiones sobre la privada. Por lo que la clave pública puede ser distribuida sin reservas por canales inseguros, como por ejemplo Internet. Mientras la clave privada siga siendo verdaderamente secreta, quedará garantizada la seguridad de la comunicación.



La encriptación asimétrica permite entregar la clave como sea.

Como al encriptar asimétricamente cada usuario posee su clave personal, este sistema cumple dos criterios de seguridad importantes:

- La *confidencialidad* queda garantizada al ser encriptados los mensajes de tal manera, que sólo pueden ser leídos por su verdadero destinatario, que deberá utilizar para eso su clave privada. Terceros quedan excluidos de la comunicación.

- La *autenticidad* la proporciona la encriptación de los mensajes con una clave privada. El destinatario puede verificar la codificación con la clave pública del remitente. Así sabrá con seguridad que el mensaje procede del supuesto remitente y ha llegado hasta él sin alteraciones.

La distribución de las claves

La difusión de las claves asimétricas es mucho más sencilla que la de sus equivalentes simétricas. La clave privada jamás debe ser dejada de la mano. Por el contrario, la pública puede ser distribuida sin problemas a través de cualquier canal. Aunque los destinatarios de las claves públicas deben aplicar ciertas medidas de seguridad. En principio, la clave pública no revela nada sobre la identidad de su propietario. Cualquiera puede crear una pareja de claves e indicar el nombre que desee. Esto hace que sea fácil enviar una clave bajo nombre falso. Por lo que antes de aceptar una clave pública, le recomendamos a usted que confirme su origen.

- Nunca acepte claves públicas que le envíen sin haberlas solicitado.
- Sea muy cauteloso con los servidores de claves públicas o los archivos de claves. Estas ofertas sólo facilitan claves para la descarga. Pero en la mayoría de los casos no garantizan la autenticidad de éstas.
- Si usted solicita que le envíen una clave pública por correo electrónico asegúrese, por ejemplo, mediante una llamada telefónica adicional, de que la clave es auténtica.

TRUCO

Servidores de claves públicas

Un modo popular de distribuir claves son los servidores de claves (*Keyserver*), que almacenan las claves públicas de los usuarios. Aunque no se debería confiar incondicionalmente en estas fuentes de claves aparentemente oficiales. Algunos servidores de claves no son más que simples archivos, en los que se puede difundir cualquier clave – es decir, aunque sea falsificada. Antes de procurarse una clave de un servidor público, le recomendamos que se informe sin falta sobre los métodos de autentificación aplicados por éste. Son muy pocos los servidores de claves, donde los usuarios se presenten personalmente, o de cualquier otra forma fiable, ante el operador del servidor, antes de que éste incluya su clave. Siempre es más seguro solicitar la clave pública directamente a su propietario. En el siguiente apartado que trata de PGP, le mostraremos cómo difundir su clave pública en un servidor de claves.

RSA – La madre de las claves asimétricas

El exponente más difundido del procedimiento de encriptación asimétrica es RSA, denominado así por sus creadores Rivest, Shamir y Adleman. En comparación con DES, RSA aplica a la encriptación métodos matemáticos bastante

más complicados. Aprovecha el hecho de que es mucho más sencillo multiplicar dos números primos, que fraccionar un producto de números primos. Usted mismo puede comprobar fácilmente este efecto. Compare el tiempo que necesita para multiplicar 13 por 23 y el que se requiere para averiguar los dos números primos que multiplicados den como resultado 289. Esta desproporción la aprovecha RSA, asignando a la encriptación una multiplicación de números primos y a la desencriptación la división en números primos. Con números de varios cientos de dígitos, la cantidad de cálculos necesarios para estas operaciones aritméticas puede dispararse rápidamente hasta el infinito. Por eso RSA no interpreta el texto legible a encriptar como secuencia de bits, sino como números grandes. También la clave es un número y se puede aplicar el mismo principio: cuanto más grande, más segura.

En RSA la clave tiene una longitud variable, de modo que el usuario la puede adaptar a sus necesidades de seguridad. Pero la desventaja de RSA – comparado con el procedimiento simétrico – es que requiere un número de cálculos claramente mayor para encriptar y desencriptar. Aquí se impone encontrar siempre un buen término medio entre seguridad y rendimiento.

INFO

¿Hasta qué punto es seguro RSA?

Con ciertas limitaciones, RSA puede ser considerado un procedimiento muy seguro. Precisamente debido a su popularidad, en el pasado tuvo que soportar infinidad de ataques de revienta-códigos serios y no tan serios. De hecho, se consiguió reventar claves RSA. Aunque, por otra parte, éstas no eran demasiado largas. Las claves más recientes de hasta 2048 bits pueden ser consideradas como seguras. Sin embargo, un punto débil de RSA estriba en sus complejos procedimientos aritméticos y la mayor dificultad que esto supone para la implementación. Aquí es fácil que los programadores cometan errores, que después aprovechen los revienta-códigos. Por ejemplo, hace algunos años se descubrió que el tiempo requerido para la desencriptación permite sacar conclusiones sobre la clave. Actualmente este peligro es eliminado mediante una pausa artificial y casual insertada en los cálculos. Pero siempre existe la posibilidad de descubrir puntos de ataque similares.

Junto con DES, RSA es la segunda gran columna que apuntala un tráfico de datos seguro. Infinidad de técnicas y productos populares las aplican, como por ejemplo PGP, S-HTTP y SSL. Es curioso que como más fuerza tienen ambas técnicas es combinadas. Frecuentemente se emplea la encriptación RSA con su profusión de cálculos, para intercambiar al comienzo de una transacción una clave simétrica de sesión más eficaz. Así se evita el problema del intercambio de claves originado por el procedimiento simétrico.

Así se revientan las claves

La ciencia de codificar datos se llama *criptografía*. Para codificar un texto legible y hacer de él un texto en clave, los criptógrafos emplean uno o varios proce-

dimientos de encriptación concretos (*Cifra*). Reventar un procedimiento recibe el nombre de *criptoanálisis*. Éste abarca varios métodos de ataque:

- En el *análisis del texto clave* el atacante sólo conoce el propio el texto en clave. A partir de éste, intentará averiguar el texto legible. Este procedimiento es el más difícil y sólo funciona con cifras muy sencillas.
- En el *análisis del texto legible* el atacante conoce tanto el texto legible como el texto en clave y, a partir de éstos, intentará averiguar la clave. Como en este caso, el agresor tiene la posibilidad de establecer conexiones entre texto legible y texto en clave, estamos ante la forma de análisis más sencilla.
- Aún resulta más fácil con el *análisis del texto legible seleccionado*. En este método el atacante no sólo conoce los textos en clave y claro, sino él mismo puede, incluso, determinar el contenido del texto legible. Esto ocurre, por ejemplo, cuando consigue furtivamente que le encripten un texto propio con el procedimiento buscado. En este caso podrá configurar el texto de tal modo que le facilite al máximo la tarea de reventar el procedimiento.
- Si estas tres variantes no conducen a nada sólo quedará ya la *Brute Force* ("fuerza bruta"). Mediante una búsqueda completa de claves, se prueban todas las claves posibles que sean aplicables al procedimiento. Desde luego, esto permite averiguar claves como las DES de 64 bits de longitud, aunque para ello se necesite concentrar toda la capacidad del ordenador y lleve mucho tiempo. Pero para reventar de esta manera claves más largas habría que superar en primer lugar algunas leyes de la física. Los ordenadores actuales deberían desplazar por sus conectores impulsos eléctricos a una velocidad superior a la de la luz, para obtener un resultado antes de que expire el ciclo vital de nuestro universo.

Por cierto, todos estos métodos presuponen que se conoce el procedimiento de encriptación verdadero y que sólo hay que averiguar la clave. Si ni siquiera se sabe cómo funciona el procedimiento, reventarlo se vuelve algunas dimensiones más difícil.

INFO

Revienta-códigos y criptógrafos

Dicho sea de paso: intentar reventar una clave no es nada ignominioso. Al contrario. Si usted lo consigue de verdad, tendrá asegurado el reconocimiento de la profesión y quizá le espere un trabajo bien pagado en la industria del software. Naturalmente, la condición indispensable es que usted publique inmediatamente sus resultados y no los aproveche clandestinamente para fines ilícitos. Y en el entorno de la Red también agradecen los intentos fracasados, si van bien documentados. Al fin y al cabo, sólo los intentos de reventar un código pueden dar información sobre su fiabilidad. Así que, ¡manos a la obra!

7.3 Lectores encubiertos, ¡no, gracias! – encriptar un e-mail con PGP

Para encriptar e-mails se ha consagrado en Internet como estándar de facto el programa ***Pretty Good Privacy*** (PGP). Traducido al español, el nombre viene a significar algo así como "entorno privado muy seguro" y ya define al programa. Inicialmente fue desarrollado por un usuario particular de Internet llamado Phil Zimmermann y pronto adquirió popularidad y apoyo en la comunidad de Internet. Por eso está disponible para prácticamente todas las plataformas y todos los sistemas operativos, lo que supone una ventaja inapreciable. Actualmente PGP es perfeccionado y comercializado a escala profesional por una importante empresa de los Estados Unidos. Pero sigue habiendo una versión gratuita del programa a la que, aunque carezca de algunas funciones complementarias, no falta ninguna de las prestaciones del programa completo, que son importantes para la seguridad. Se puede descargar en http://www.pgpinternational.com.

PGP trabaja con las claves asimétricas seguras basadas en los procedimientos RSA o Diffie-Hellman/DSS. Mientras las versiones anteriores a la 5.0 sólo trabajaban bajo DOS y necesitaban interfaces de Windows adicionales, las versiones más recientes (a partir de la 5.0) para Windows al fin se ajustan a los tiempos actuales y son cómodas. Aparte de una interfaz de fácil manejo disponen, además, de unos prácticos plug-ins con los que PGP se integra sin problemas en los programas de correo electrónico habituales, como por ejemplo Outlook Express. Esto hace de la encriptación y desencriptación un juego de niños. En las siguientes páginas vamos a mostrarle el manejo de PGP, primero mediante Outlook Express. Pero la aplicación de PGP no queda limitada únicamente a este programa, por lo que después explicaremos cómo emplear PGP de un modo práctico con cualquier programa de comunicación.

Las herramientas de PGP

PGP es un software potente y flexible compuesto por varios módulos, que pueden ser arrancados y empleados en función de cada tarea. Para que usted pueda seguir mejor las instrucciones que le daremos a continuación, primero vamos a resumir brevemente el manejo del programa.

PGPtray – el icono de PGP de la Bandeja de sistema

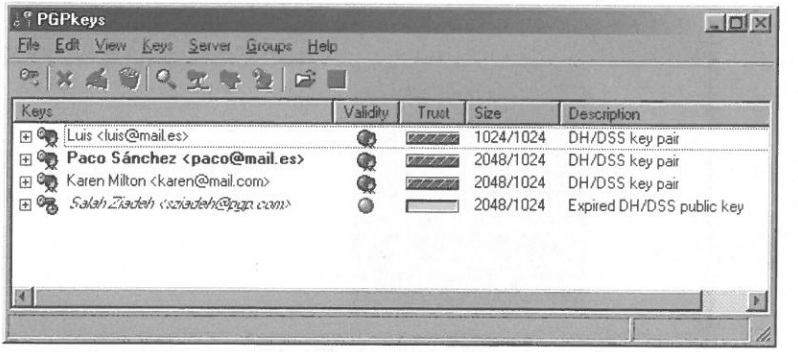
Después de la instalación usted verá en el margen inferior derecho de la Bandeja de sistema de su PC, un nuevo icono llamado *PGTray*. Indica que PGP está activo en su ordenador y, aparte de esto, facilita directamente las funciones más importantes al hacer clic sobre el icono con el mouse. Desde aquí, aparte de la ayuda y las opciones, se pueden ejecutar los demás módulos de PGP *PGPkeys* y

PGPtools. Además, el menú contiene abreviaturas de las funciones más importantes para encriptar y desencriptar el contenido de ventanas actuales o del Portapapeles.

El icono PGPtray en la Bandeja de sistema proporciona acceso a las funciones más importantes.

PGPkeys – la administración de claves

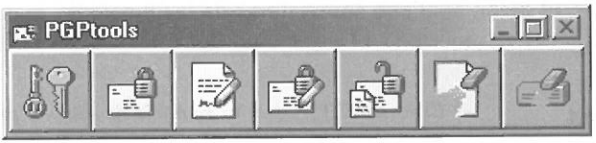
Otro módulo importante es *PGPkeys*. Este programa es responsable de administrar las claves de PGP. Desde aquí usted puede crear sus propias claves y distribuirlas a otros usuarios. También se importan aquí las claves ajenas, o se pueden buscar selectivamente las claves públicas de otras personas.



PGPkeys administra las claves propias y las públicas de otros usuarios.

PGPtools – el centro de control

PGPtools es el centro de control. Adquiere importancia, sobre todo, si no se usa ningún programa de correo electrónico que permita emplear directamente las funciones de PGP mediante plug-in. En este caso, mediante clic del mouse PGPtools pondrá a su disposición todas las funciones de PGP necesarias, en una pequeña ventana con siete botones. En las siguientes páginas nos dedicaremos en detalle a las diferentes funciones de PGP.



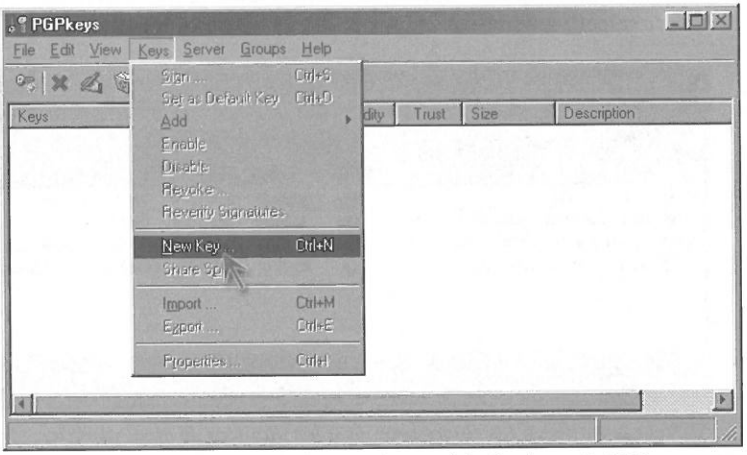
El centro de control de PGP: PGPtools.

Crear una clave PGP propia

Para comunicarse con seguridad a través de PGP usted necesitará, en primer lugar, su propia pareja de claves. En este apartado vamos a mostrarle los pasos necesarios para obtenerlas.

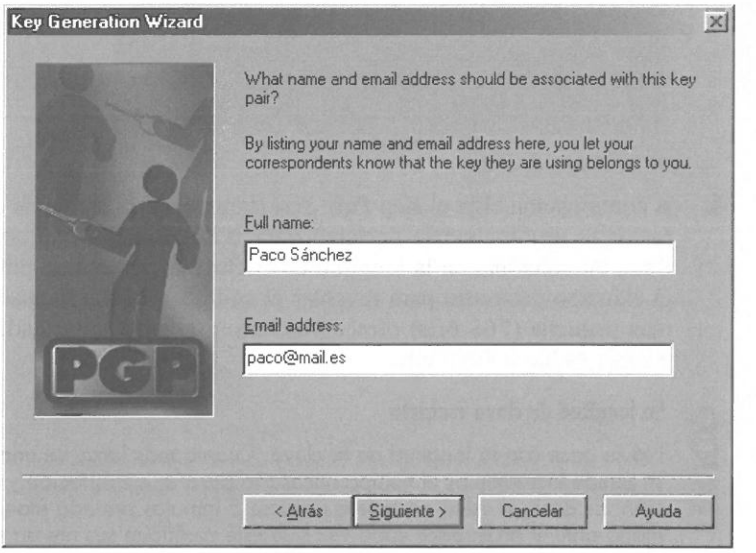
Para la creación de su propia pareja de claves *PGP*, un ayudante automático, el *asistente de creación de claves*, le guiará por todos los pasos. Lo encontrará en el programa de administración *PGPKeys*, que deberá llamar con *Inicio/Programas/PGP/PGPKeys* o, si está en Outlook Express, con *Herramientas/PGP/PGPKeys*.

1. Arranque el asistente con *Keys/New Key* ... dentro del programa de administración *PGPKeys*.



Con Keys/New Key, llama al asistente de creación de claves de PGP.

2. Como primer paso indique su nombre y su dirección de correo electrónico. En principio, aquí puede introducir los datos que desee. Pero como éstos serán transmitidos a su compañero de comunicación junto con la clave pública, sería conveniente que elija denominaciones útiles e inequívocas.



Indique su nombre y su dirección de correo electrónico.

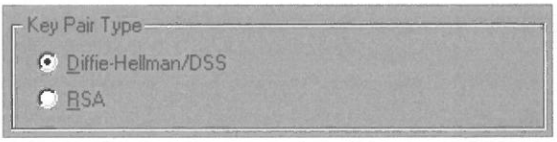
3. En el segundo paso decídase por una *Key Pair Type* (pareja de claves) entre dos alternativas posibles. Aquí dispone de:

- *Diffie-Hellman/DSS* es el nuevo procedimiento de encriptación de PGP. Es el que se recomienda a los usuarios y también será soportado por las versiones futuras. Le aconsejamos que se decida generalmente por esta técnica. Aunque, por otra parte, si la elige no se podrá comunicar con los usuarios de versiones más antiguas de PGP.
- *RSA* es el procedimiento de encriptación antiguo y clásico. Era empleado exclusivamente por versiones anteriores de PGP, pero la intención de su fabricante es sustituirlo en el futuro por Diffie-Hellman/DSS. No hay ninguna certeza de que las versiones futuras de PGP sigan soportando este procedimiento. Usted sólo debería decidirse por esta técnica si sus compañeros de comunicados aún trabajan con las versiones antiguas de PGP y no están dispuestos a actualizarse.

TRUCO

Dos claves paralelas

Si usted no consigue decidirse por uno de los dos procedimientos, ¿por qué no emplea ambos? En principio, con PGP puede crear todas las claves que quiera aplicando cualquiera de las dos técnicas. Por lo tanto, puede crear una clave Diffie-Hellman/DSS y una clave RSA. Aunque, en ese caso, deberá controlar a quién entregó determinadas claves públicas y qué clave pública deberá emplear para encriptar los datos de cada destinatario.



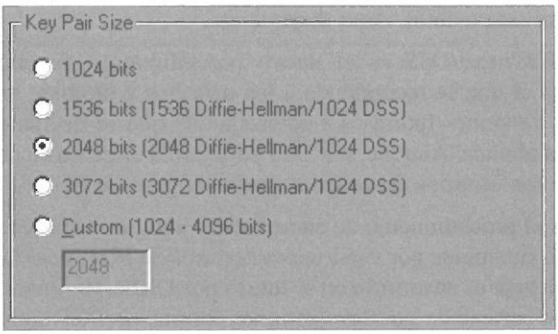
Elija el tipo de clave.

4. A continuación elija el *Key Pair Size* (tamaño de la pareja de claves). Este factor es absolutamente decisivo para la seguridad de su comunicación. Cada bit adicional en la longitud de la clave incrementará potencialmente el esfuerzo necesario para reventar el código. Aunque incluso la longitud más pequeña (*768 bits*) ofrece ya cierto grado de seguridad. El máximo posible es hasta 4096 bits.

TRUCO

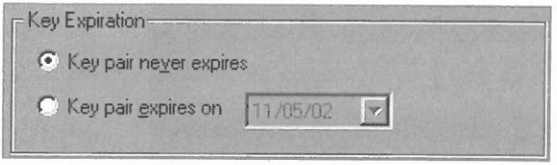
La longitud de clave correcta

No se pase con la longitud de la clave. Cuanto más larga es una clave más se puede incrementar el tiempo necesario para la encriptación y desencriptación. Es decir, si usted no quiere pasarse 5 minutos sentado mano sobre mano ante el ordenador cada vez que este codifique sus mensajes, debería elegir un valor intermedio. 1024 a 2048 bits ya suponen un aceptable término medio entre seguridad y rendimiento.



Decida la longitud y, con ella, la fiabilidad de la clave.

5. Si quiere que su clave siga vigente hasta que usted mismo la retire de la circulación, elija en el siguiente paso la opción *Key pair never expires*. Si, por el contrario, lo que desea es indicar una fecha en la que la clave deba ser desactivada automáticamente, seleccione la opción *Key pair expires on ...* e introduzca en el campo que viene a continuación la fecha de caducidad.



Decida si la vigencia de la clave debe ser ilimitada.

INFO

Plazo de vigencia de las claves

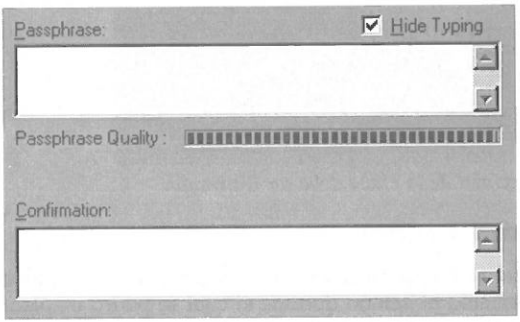
Para cada clave se puede establecer una *Key Expiration (Vigencia de clave)*. Esta fecha determina el tiempo durante el cual se podrá emplear una clave para encriptar y firmar. Una vez transcurrida esa fecha la clave sólo servirá para desencriptar y comprobar firmas. Para la comunicación normal no es imprescindible decidir una fecha de caducidad. El empleo de una nueva clave siempre trae consigo algunas molestias, hasta que todos los implicados en la comunicación hayan recibido la clave pública nueva y la empleen. Por eso sólo le recomendamos dar este paso, si sospecha que su clave ha caído en manos no autorizadas. Las claves de caducidad automática convienen sobre todo a usuarios con grandes necesidades de seguridad. Así serán obligados de modo automático a crear regularmente una nueva clave y ponerla en circulación. Si alguien hubiera conseguido averiguar la clave antigua pese a todas las precauciones, esto hará que deba empezar de nuevo.

6. Cada clave privada va protegida con una *Passphrase* (frase de paso o contraseña). Sólo se puede emplear una clave privada para encriptar o desencriptar, si ha sido introducida esta frase. Naturalmente, el término frase contraseña sólo es otra expresión para palabra clave, con la que se pretende evidenciar que una expresión compleja (como una frase completa) es más segura que una palabra suelta. Introduzca para su clave en el campo *Passphrase* una contraseña segura. Repita la entrada más abajo, en el campo *Confirmation* para evitar errores mecanográficos. El indicador *Passphrase Quality* situado entre los dos campos le revelará lo segura que es la palabra clave seleccionada. Esto depende de la longitud de la entrada y de los caracteres empleados. Los caracteres especiales como, por ejemplo "!/?()§&$", hacen que su frase contraseña sea considerablemente más segura. Ya hemos explicado a fondo en el Capítulo 2, cómo elegir una contraseña segura.

TRUCO

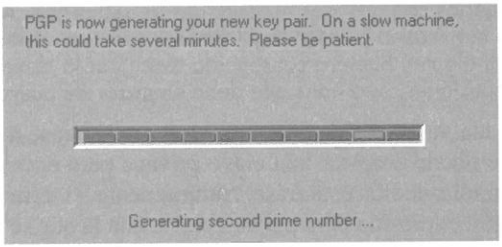
Visualizar la palabra clave

Si usted prefiere ver lo que teclea desmarque la casilla *Hide Typing* (ocultar escritura). Aparecerán en pantalla los caracteres tecleados. Pero cuando aplique este procedimiento vigile, sobre todo, que nadie le observe por encima del hombro mientras introduce los datos.



Proteja su clave con una frase contraseña segura.

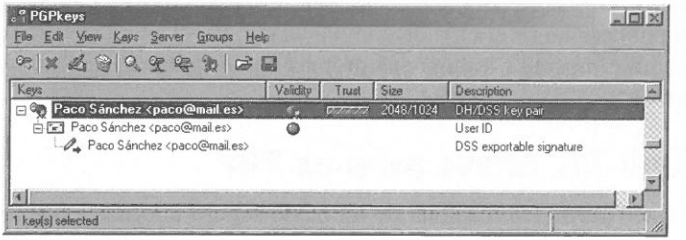
7. Ahora PGP posee todos los datos que necesita. En el siguiente paso tendrá lugar la creación de la pareja de claves utilizando estos datos. Puesto que se trata de un proceso de cálculo matemático bastante complicado, según la velocidad del ordenador podrá tardar algún tiempo.



PGP calcula la nueva pareja de claves.

8. Con esto usted ha creado su nueva pareja de claves. Para concluir el proceso dispone de la posibilidad de divulgar su nueva clave pública en un servidor de claves. Éste almacena las claves públicas de muchos usuarios de PGP. Si usted también desea distribuir su clave pública de este modo, PGP la transmitirá directamente al servidor. Establezca para eso una conexión con Internet y active la opción *Send my key to the root server now* (enviar mi clave al servidor raíz ahora), antes de hacer clic sobre *Siguiente*. Pero tenga en cuenta que al hacer esto perderá el control sobre quién emplea su clave pública, y también para sus compañeros de comunicación será más seguro si reciben la clave directamente de usted. A fin de cuentas, cualquiera podría distribuir con el nombre de usted una clave pública en el servidor de claves.

Con esto, queda concluido el proceso para crear una nueva pareja de claves. Desde este momento encontrará en el gestor de claves de PGP (*PGPkeys*) la entrada correspondiente a su clave.



La nueva pareja de claves es visualizada en el gestor de claves.

Para cada clave almacenada, el administrador de claves PGPKey proporciona diferentes tipos de información:

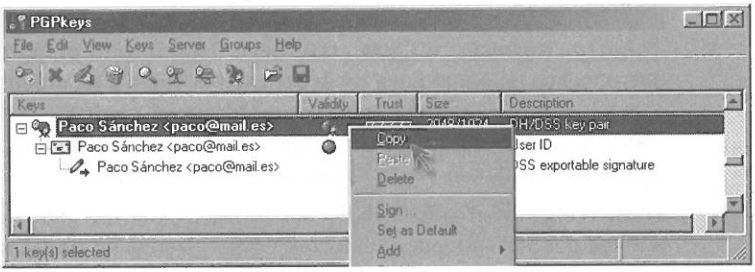
- *Keys (claves)* – La denominación de la clave, compuesta por un símbolo, el nombre y la dirección de correo electrónico del propietario. Los símbolos gráficos tienen distintos significados. Las llaves amarillas representan a las claves Diffie-Hellman/DSS más recientes, mientras las azules se refieren a las claves RSA obsoletas. Reconocerá sus propias claves por el icono de doble llave.
- *Validity (vigencia)* – Cada clave tiene determinado grado de confianza, que depende de cómo haya recibido usted la clave y de quién. Los círculos y cuadrados verdes significan que usted puede confiar totalmente en esa clave. Los símbolos grises advierten de confianza restringida. En estas claves la procedencia no es del todo clara.
- *Trust (confianza)* – Este indicador le informa si una persona cuya clave pública posea usted, puede autorizar como persona de confianza la clave de terceros y hasta qué límite. Si usted recibe una clave pública firmada adicionalmente por una de sus personas de confianza, ésta será considerada como digna de confianza. Esto se manifiesta por un indicador de confianza verde.
- *Size (tamaño)* – En este campo se indica el tamaño de una clave, es decir, el número de bits empleados en la encriptación. Cuanto mayor sea el número más segura será la clave. En las nuevas claves Diffie-Hellman/DSS encontrará siempre una información para la parte Diffie-Hellmann y otra para la parte DSS de la clave.
- *Description (descripción)* – La descripción abreviada explica las diferentes entradas pertenecientes a una clave. Aparte de la verdadera entrada de una clave, usted podrá abrir más entradas subordinadas haciendo clic con el mouse sobre el signo "+", igual que ocurre en Explorer. Estas subentradas contienen, por ejemplo, uno o varios identificadores de usuario que vayan asignados a una clave. Cada clave también posee una parte pública y exportable, que usted podrá transmitir a otros usuarios.

El gestor de claves sirve para que usted administre su propia pareja de claves y las claves públicas de su círculo de comunicación. En el siguiente capítulo describimos cómo transmitir a otros sus propias claves públicas con la ayuda del gestor de claves.

Distribuir las claves propias PGP

Para que usted pueda intercambiar de un modo seguro información y datos con sus compañeros de comunicación, estos deberán conocer en primer lugar la clave pública de usted. Como la clave pública no pone en peligro la seguridad de su clave privada, podrá distribuirla sin problemas por medios como el correo electrónico.

1. Para ello marque la entrada de su pareja de claves en el gestor de claves.
2. Abra el correspondiente menú contextual haciendo clic con el botón derecho del mouse. Allí encontrará la opción *Copy*, que le permitirá trasladar la clave pública al Portapapeles.



Traslade la parte pública de su clave PGP al Portapapeles.

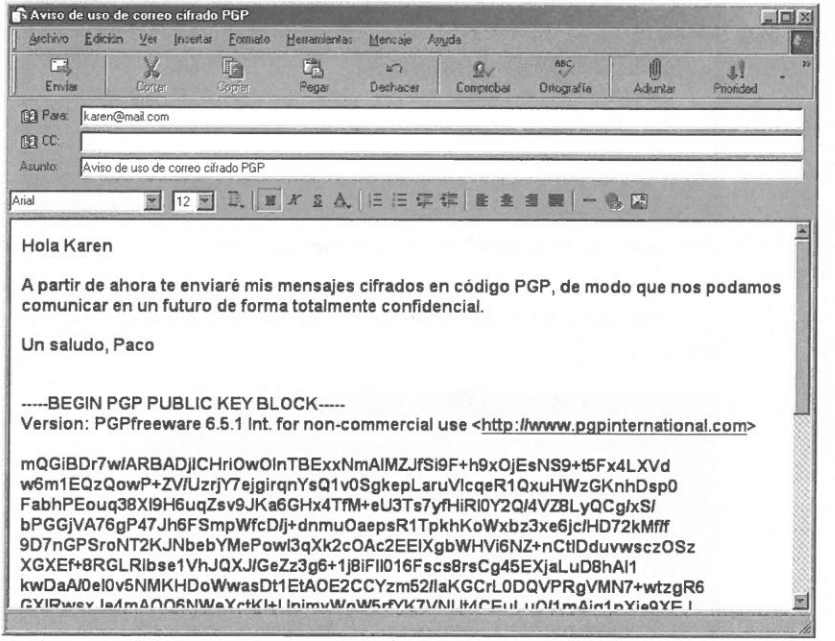
INFO

¿Existe la posibilidad de que yo mismo publique por error mi clave privada?

No se preocupe por su clave privada. PGP no permite que sea transmitida por accidente. Aunque usted la marcara e hiciera clic en *Copy*, PGP sólo divulgaría la parte pública de ésta.

3. Abra ahora su programa de correo electrónico y redacte un mensaje al o los receptores de su clave. Explíqueles brevemente de qué trata. Quizá sea bueno añadir al mensaje una nota, que demuestre al destinatario que el e-mail procede realmente de usted.
4. Ahora, vuelta a utilizar en la ventana de texto el botón derecho del mouse. En el menú contextual encontrará la función *Paste* o *Pegar*. También existe la alternativa de llamar a esta función desde el menú *Edit* o *Edición*. Este comando inserta el contenido del Portapapeles en el mensaje.

5. Envíe el mensaje como de costumbre. Los destinatarios podrán extraer la clave pública del mismo e insertarla en su libreta de claves.

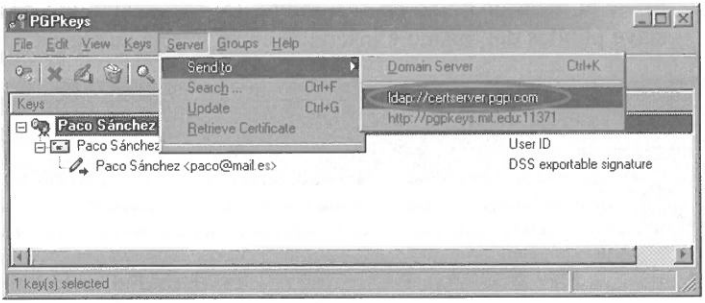


Así se inserta una clave pública en un e-mail.

Publicar la clave en un servidor de claves

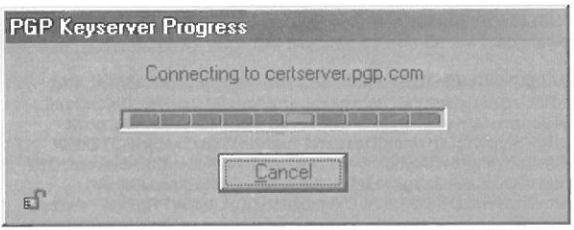
Para que otras personas puedan enviarle escritos confidenciales sin haberse puesto antes en contacto con usted existen los servidores de claves. Éstos ponen a disposición grandes archivos con claves públicas de usuarios de PGP de todo el mundo. Para que también figure en ellos su clave, usted la deberá transmitir al servidor de claves. Proceda del siguiente modo:

1. Marque su clave en el gestor de claves *PGPkeys*.
2. Seleccione la función de menú *Server/Send to*. En el submenú, elija uno de los servidores disponibles. *certserver.pgp.com* es el servidor de claves oficial de PGP. Aparte de él, también existen otros servidores de diferentes proveedores. Usted también puede publicar su clave en varios servidores, para lo cual deberá repetir este proceso por cada uno de ellos.



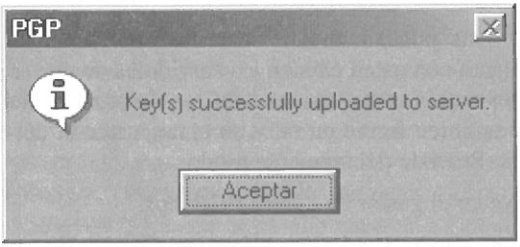
Haga publicar su clave PGP en un servidor de claves.

3. Ahora *PGPkeys* establecerá contacto con el servidor de claves seleccionado y, una vez conectado, el programa transmitirá la clave pública a ese servidor.



PGP establece contacto con el servidor de claves seleccionado.

4. Si la clave ha podido ser publicada correctamente en el servidor, *PGPkeys* lo confirmará con un mensaje de consecución.

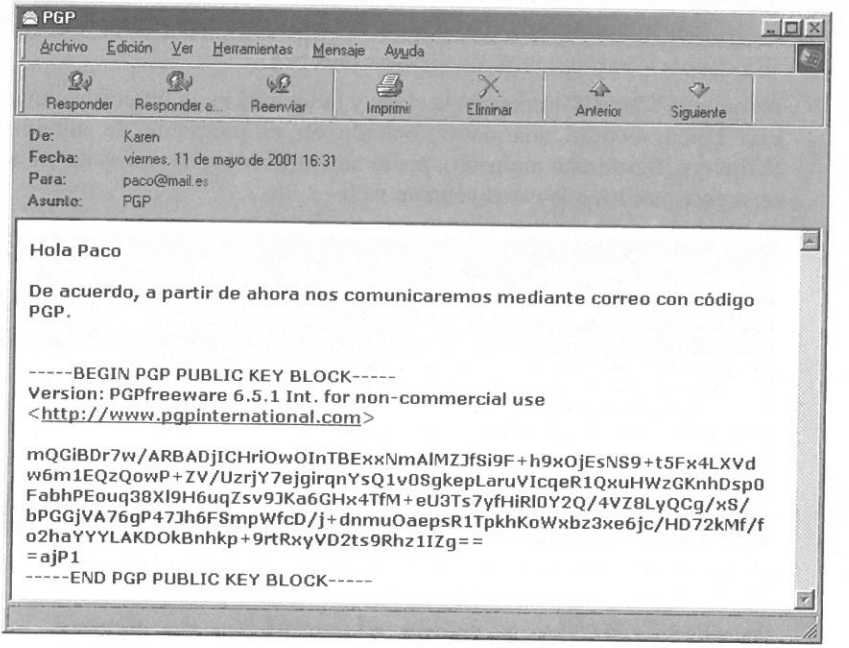


La clave fue publicada correctamente.

Desde este momento la clave estará disponible en el servidor. En el siguiente apartado vamos a mostrarle cómo puede usted buscar una clave pública en un servidor de claves e incluirla en su libreta de claves.

Incluir claves públicas

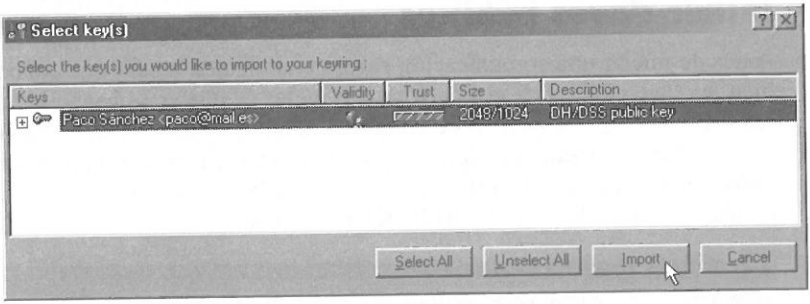
Antes de iniciar una comunicación segura con alguien tendrá que conocer también la clave pública de esa persona. Lo mejor es que se la haga enviar por e-mail. Cuando un compañero de comunicación le mande a usted su clave pública, por ejemplo mediante correo electrónico, inclúyala en su libreta de claves. Usted reconocerá si el mensaje contiene claves PGP, por la línea inicial característica "----- BEGIN PGP PUBLIC KEY BLOCK -----".



Un e-mail con una clave PGP pública.

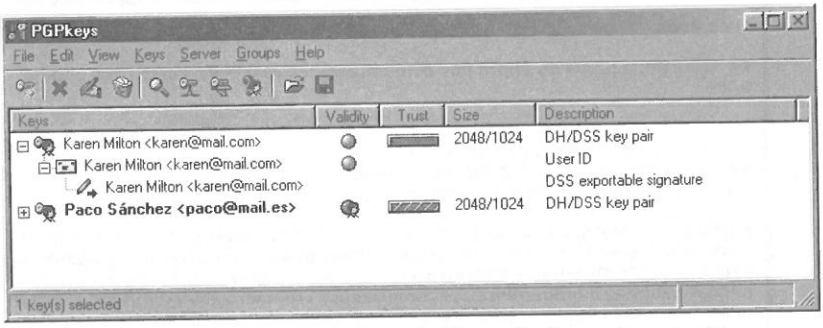
1. Abra el e-mail con doble clic de modo que el mensaje aparezca en una ventana propia (¡no en la vista previa!).
2. Haga clic sobre el icono de *Decrypt PGP...* (desencriptar mensajes PGP) de la barra.

3. Ahora PGP le mostrará las claves públicas contenidas en el mensaje. Por regla general sólo suele haber una. Si hubiera varias claves usted podrá elegir entre ellas la que quiera aceptar.



Seleccione la o las claves públicas que desee importar.

A continuación PGP importará la clave y la incluirá en la libreta de claves públicas. Usted recibirá una nueva entrada en el programa de administración PGPKeys. Desde este momento, podrá autentificar los mensajes de ese remitente, o encriptar los que usted le envíe a él.



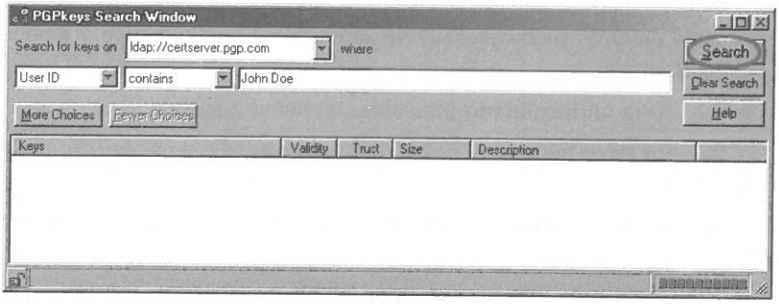
La clave pública importada es incluida en la libreta de claves almacenadas.

Importar la clave desde el servidor de claves

Aparte de recibir una clave pública de su propietario o de otra persona de confianza, existe otro camino para obtener las claves públicas ajenas. En los grandes servidores de claves se ofrecen archivos con claves públicas de usuarios PGP. PGPKeys le permite explorar estos archivos e importar las claves halladas:

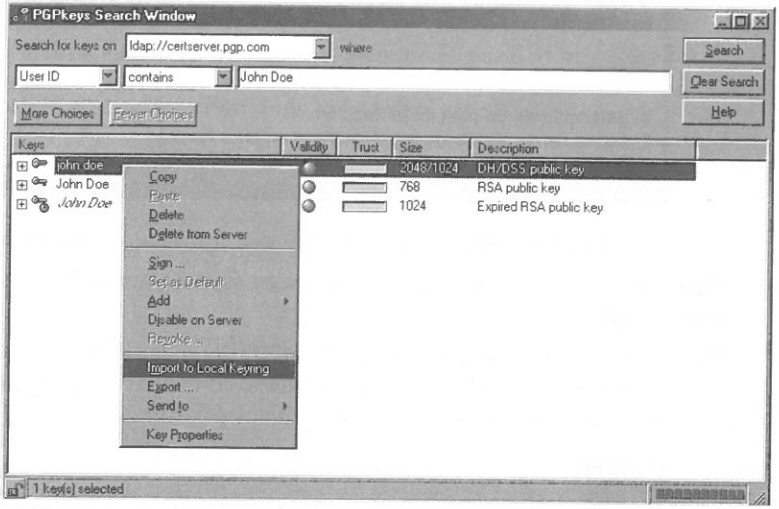
1. Llame en el programa de administración PGPKeys la función *Server/Search*.
2. En la ventana de búsqueda de PGPkeys (*PGPkeys Search Window*), formule ahora una consulta. Seleccione en primer lugar el servidor de claves donde quiera buscar. Por regla general, la mejor elección quizá sería el servidor de claves oficial de PGP *ldap://certserver.pgp.com*.
3. Para buscar el nombre de una persona seleccione en el campo situado a la izquierda del todo la opción *User ID*.

4. En el campo de selección situado a la izquierda de éste configure *contains*.
5. Finalmente, introduzca a la derecha del todo el nombre de la persona buscada e inicie la búsqueda haciendo clic sobre el botón *Search*.



Así puede buscar las claves públicas de PGP.

6. Acto seguido PGPKeys buscará en el servidor de claves las claves públicas cuyo User-ID contenga el nombre indicado. Después de un rato, le presentará la lista de las claves halladas.
7. Para incluir una de estas en su libreta de claves haga clic sobre la entrada con el botón derecho del mouse. En el menú contextual encontrará el comando *Import to Local Keyring*. Esta función le permitirá importar la clave desde el servidor.

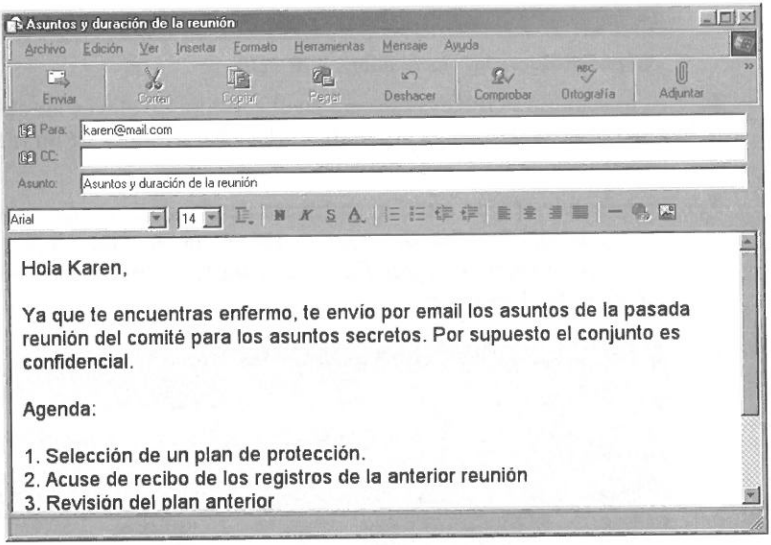


Así importa usted desde el servidor de claves las claves halladas.

Encriptar mensajes

Inicialmente, la creación de un mensaje no se distingue del modo de proceder habitual. Es decir, usted redactará el mensaje como siempre. Sólo tendrá que indicar, además, que esa misiva debe enviarse encriptada. Entonces, antes de que usted envíe el mensaje, PGP se activará automáticamente y se encargará de la encriptación.

1. Abra un formulario para crear un nuevo mensaje.
2. En *Para* indique el destinatario del mensaje y en *Asunto* de qué trata el e-mail.
3. Ahora introduzca en el campo de texto el contenido del mensaje.



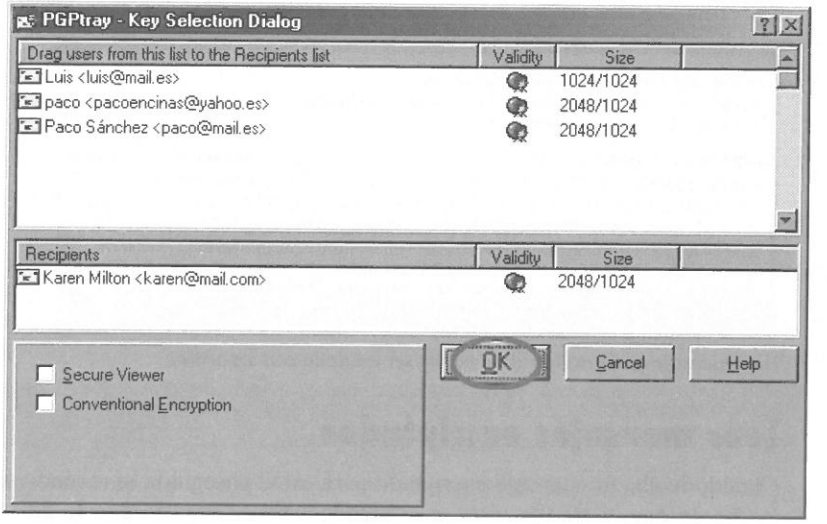
Inicialmente redacte el mensaje confidencial siguiendo el procedimiento habitual.

Hasta aquí no ha cambiado nada. Ahora es cuando vienen los pasos decisivos para encriptar.

4. Haga clic sobre el botón *Encrypt PGP* (Encriptar PGP) situado en la barra de botones de Outlook Express. Con eso comunicará al plug-in de PGP que este mensaje deberá ser encriptado antes de su envío.

5. A continuación haga clic como siempre sobre el botón *Enviar* para mandar el mensaje.

Esto activa el plug-in. Si es posible asignar inequívocamente una clave pública al destinatario indicado en la línea *Para*, el programa encriptará el mensaje de modo totalmente automático para ese destinatario. De lo contrario le mostrará a usted la libreta de claves públicas y le pedirá elegir al destinatario (o destinatarios) para el que deba ser encriptado ese mensaje.



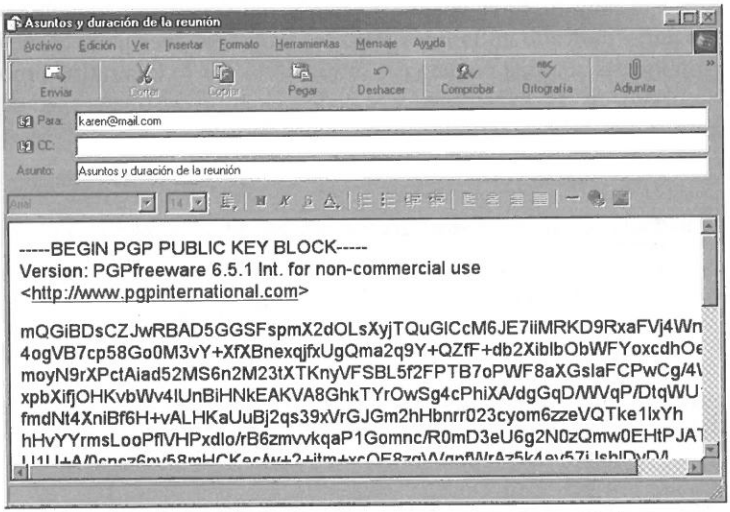
Seleccione el destinatario del mensaje confidencial.

6. Seleccione al o los destinatarios y confirme su elección con OK. Ahora el plug-in de PGP encriptará el mensaje. Después sustituirá el texto legible original del mensaje por su réplica encriptada y colocará el mensaje en la bandeja de salida correo. Si usted quiere cerciorarse de este proceso, allí puede volver a abrir el mensaje y verlo.

TRUCO

Encriptar mensajes para usted mismo

Cuando usted encripte un mensaje con la clave pública de un destinatario éste ya sólo podrá ser leído con la clave privada de éste. Es decir, ni usted mismo podrá reconocer el mensaje que haya escrito. Si quiere archivar los mensajes enviados para poder releerlos más adelante siempre que quiera, esto no resulta nada práctico. Por suerte, PGP le puede ayudar. Abra la configuración de PGP con *Edit/Options...* y pase a la pestaña *General*. Active la opción *Always encrypt to default key* (Encriptar siempre con clave estándar) y confirme esta opción con *Aceptar*. Esto hará que cuando PGP encripte un mensaje lo codifique también automáticamente para la clave privada de usted. Así, después podrá ver sus propios e-mails cuando quiera.



Este mensaje está encriptado y puede ser enviado con seguridad.

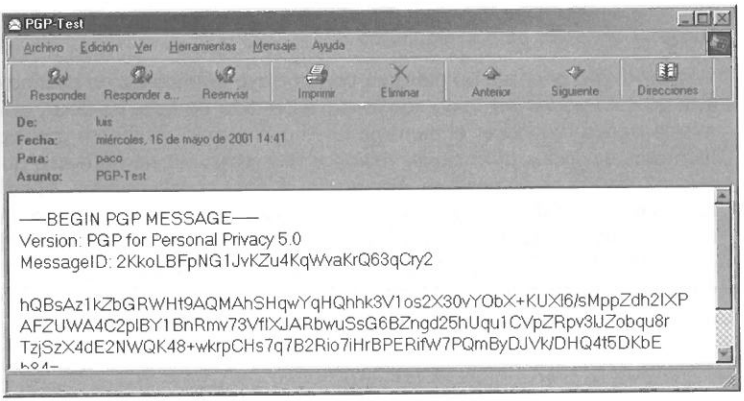
Leer mensajes encriptados

Cuando reciba un mensaje encriptado para usted enseguida lo reconocerá por el hecho de que, a simple vista, no entenderá nada. Pero lo que le advertirá de modo inequívoco es la línea característica

----- BEGIN PGP MESSAGE -----

seguida de la versión del software PGP empleado. Todo lo que venga después será un mensaje encriptado. Finaliza con la línea

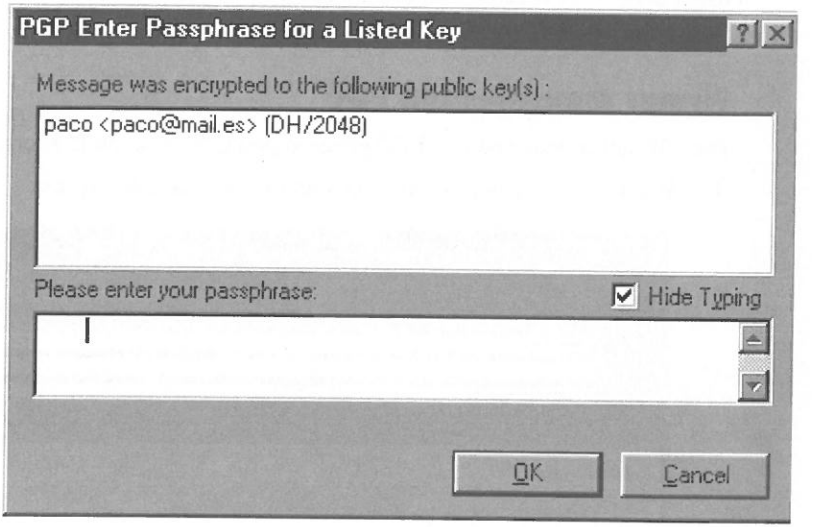
----- END PGP MESSAGE -----



Este es el aspecto que tiene un mensaje recibido con encriptación PGP.

1. Cuando reciba un mensaje encriptado haga clic sobre el botón *Decrypt PGP*. El plug-in analizará el mensaje encriptado y averiguará de quién y para quién fue codificado. Si el mensaje va codificado con la clave pública de usted podrá convertirlo en legible con su equivalente privado.

2. Siempre que quiera emplear su clave privada deberá introducir primero la frase contraseña. Esto garantiza que su clave no sea utilizada por personas no autorizadas.



Introduzca la contraseña de su clave privada.

3. PGP desencriptará ahora el contenido del mensaje y sustituirá el texto codificado por otro que usted podrá leer.

Firmar mensajes

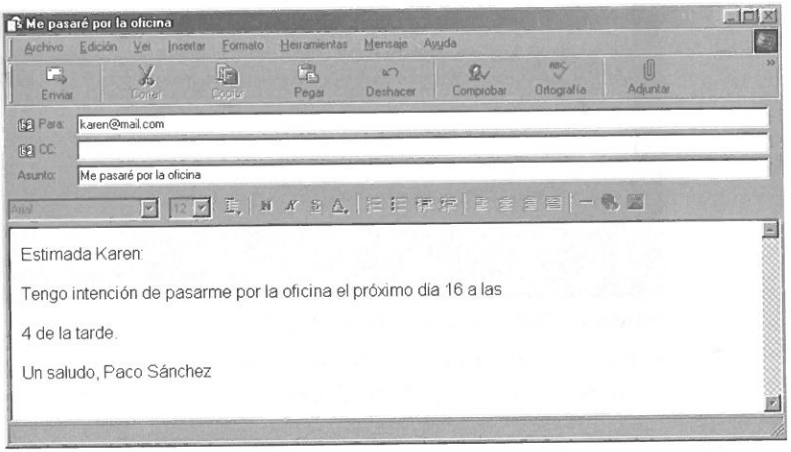
Con la encriptación de mensajes descrita en el apartado anterior queda garantizada la confidencialidad de la comunicación. Aparte del remitente y el destinatario nadie más puede leer los mensajes encriptados. Pero este método sigue teniendo un punto débil: la autenticidad de una misiva no puede asegurarse. Cualquiera que posea la clave pública del destinatario podrá encriptar un mensaje dirigido a él, y el receptor no podrá comprobar si el autor del mensaje ha dado su nombre verdadero o se ha hecho pasar por otra persona.

Pero PGP también permite garantizar la autenticidad usando un truco asombrosamente sencillo. Para encriptar un mensaje se emplea siempre la clave pública del destinatario. Como el mensaje sólo puede ser descodificado con la clave privada, únicamente el destinatario legítimo podrá leerlo en texto legible. Dando la vuelta a este principio usted podrá firmar los e-mail de un modo fiable. Los mensajes que usted haya codificado con su clave privada pueden ser descifrados con la clave pública. Como es posible que esa clave pública la posean muchos compañeros de comunicación, ésta servirá de poco para mantener la confidencialidad. Sin embargo, todo destinatario que desencripte un mensaje de usted con su clave pública sabrá que esa misiva sólo ha podido ser codificada con la clave privada de usted. Como, normalmente, nadie más puede poseer esa clave privada, usted deberá ser el remitente auténtico. Este método para demostrar la autenticidad de un mensaje se llama "firma" o "firmar".

Firmar mensajes con PGP

Para firmar un mensaje con PGP primero proceda como en la encriptación.

1. Redacte el mensaje como de costumbre en Outlook Express.

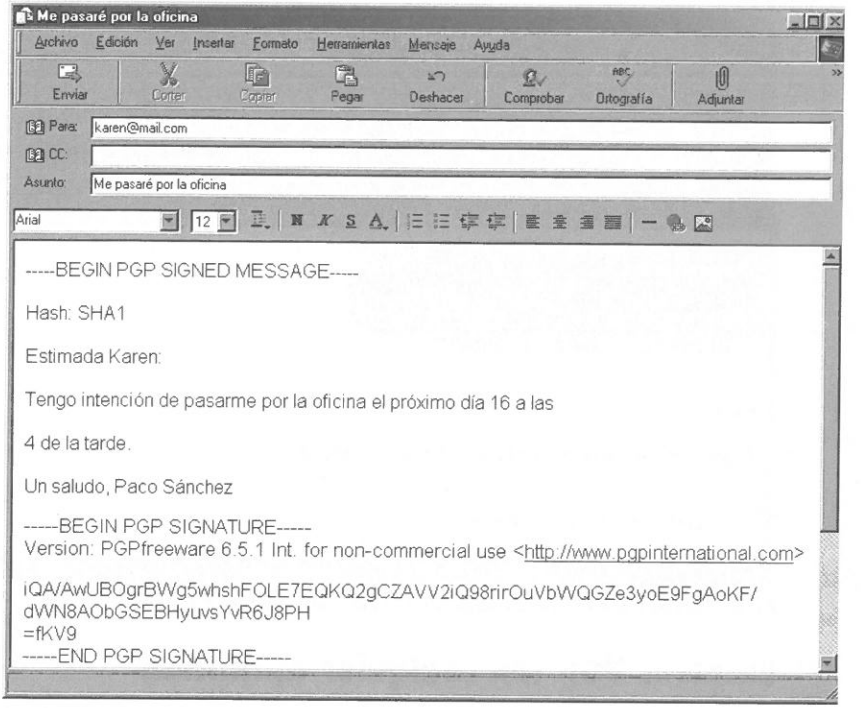


De nuevo, redacte del modo habitual el mensaje a firmar.

2. En lugar de activar el botón *Encrypt PGP* como se hace para encriptar, esta vez haga clic sobre *Sign PGP*.

Cuando haga clic sobre el botón *Enviar*, PGP dotará al mensaje de su clave privada. Para eso deberá introducir la contraseña con la que tenga protegida a su clave contra uso ilícito.

Como verá esto no encripta el mensaje, que sigue estando en texto legible. La firma sólo sirve para confirmar la autenticidad, no para proteger la confidencialidad. El destinatario necesitará la clave pública de usted para poder verificar la firma añadida al mensaje. Con esto sabrá que el mensaje es realmente de usted y quedará garantizada la autenticidad de la misiva.



Este es el aspecto que tiene un mensaje firmado.

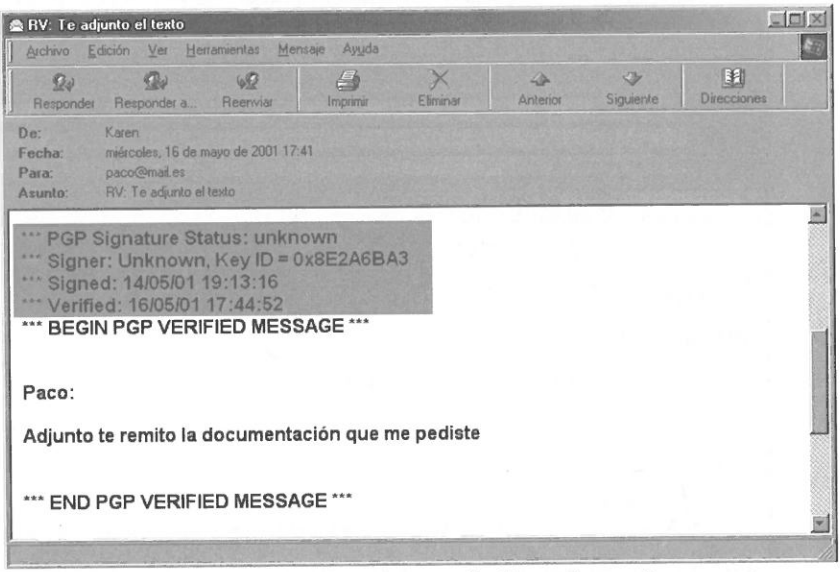
TRUCO

Encriptar y firmar

Para ir totalmente a lo seguro usted no sólo puede encriptar un mensaje sino también firmarlo. El mensaje es codificado primero con la clave pública del destinatario. Después, la misiva encriptada resultante es firmada con la clave privada del remitente. Así quedan garantizadas tanto la confidencialidad como la autenticidad de un mensaje. Para encriptar y firmar simultáneamente un mensaje con PGP, primero redáctelo como de costumbre en Outlook Express. A continuación haga clic tanto sobre el botón *Encrypt PGP* como sobre el botón *Sign PGP*. Cuando envíe el mensaje introduzca la contraseña de su propia clave privada para que PGP pueda firmar la misiva. Al encriptar y firmar usted combina las dos importantes funciones de seguridad de PGP, con lo que prácticamente excluye todos los riesgos.

Verificar las firmas

Cuando reciba un mensaje firmado proceda del mismo modo que para descodificar una encriptación. PGP detecta automáticamente si un mensaje está firmado. A continuación insertará delante de éste una breve información sobre el estado, que le revelará a usted lo siguiente:



En la información de estado usted puede ver quién firma el mensaje.

Emplear PGP con cualquier aplicación

Hasta ahora le hemos presentado las funciones más importantes de PGP con Outlook Express. Para éste y algunos otros populares programas de correo electrónico existen plug-in especiales de PGP, que permiten integrar las funciones de PGP directamente en la interfaz de los programas. Desgraciadamente esto sólo ocurre con relativamente pocos programas. Pero quien no quiera o no pueda (por ejemplo, si es cliente de un servicio on-line y no puede elegir el programa de correo electrónico) utilizar ninguno de estos programas, tampoco tiene porqué renunciar a la confidencialidad e integridad de su comunicación por correo electrónico. Bajo Windows, el Portapapeles sirve para intercambiar datos entre distintas aplicaciones. Esto también lo aprovecha PGP. El modo de proceder es el siguiente:

1. En primer lugar hay que marcar el texto cifrado o legible a encriptar, trasladándolo después al Portapapeles.
2. A continuación hay que dar instrucciones a PGP para que procese el texto contenido en el Portapapeles, es decir, que lo desencripte o encripte, según cada caso.
3. PGP analiza el texto, pide la contraseña de la clave privada si fuera necesario y lo procesa.
4. Acto seguido sustituye en el Portapapeles el texto original por la versión procesada. De este modo un texto legible se convierte en un código encriptado o uno cifrado se transforma de nuevo en texto legible.
5. Ahora usted puede reintegrar el texto desde el Portapapeles en el programa de correo electrónico. Si su programa no dispone de ninguna función para insertar textos en los mensajes recibidos, también puede leer el resultado directamente en el Portapapeles.

Aprovechar PGPTray

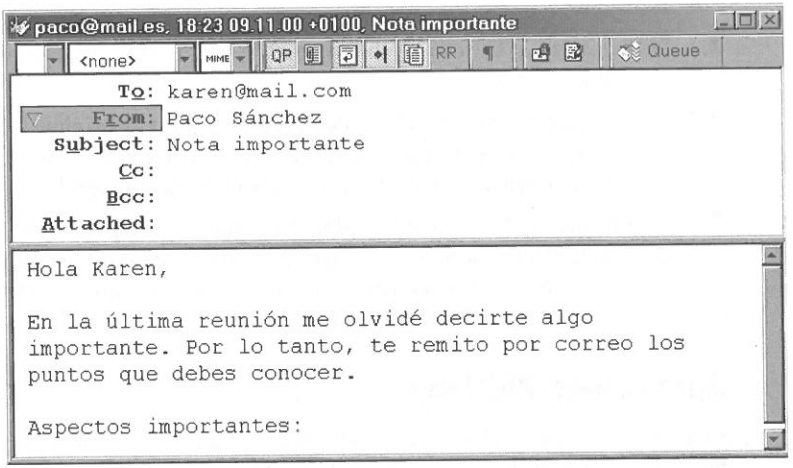
Cuando se utiliza PGP a través del Portapapeles *PGPTray*, es decir, el icono de PGP situado en el margen derecho de la Barra de tareas, adquiere importancia relevante. Como el programa de correo electrónico no soporta directamente PGP, usted no puede activar las diferentes funciones como desencriptar y encriptar desde los botones o menús del programa. En lugar de eso deberá utilizar el menú contextual de PGP Tray. Para abrirlo haga clic con el botón izquierdo o derecho del mouse sobre el icono de PGPTray de la Bandeja de sistema. En el menú encontrará reunidas las funciones de PGP más importantes.

A través del icono de PGPTray de la Barra de tareas se puede acceder rápidamente a todas las funciones importantes.

Encriptar a través del Portapapeles

Para ilustrar cómo funciona queremos mostrarle mediante un ejemplo concreto el modo de encriptar un mensaje con PGP a través del Portapapeles.

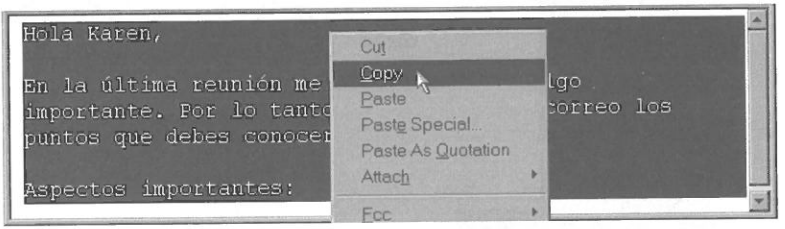
1. Para enviar un mensaje encriptado primero redáctelo del modo habitual con su programa de correo electrónico. No será necesario que tenga en cuenta ninguna particularidad cuando ponga las señas ni cuando escriba el texto del mensaje.



En primer lugar se redacta el mensaje como de costumbre.

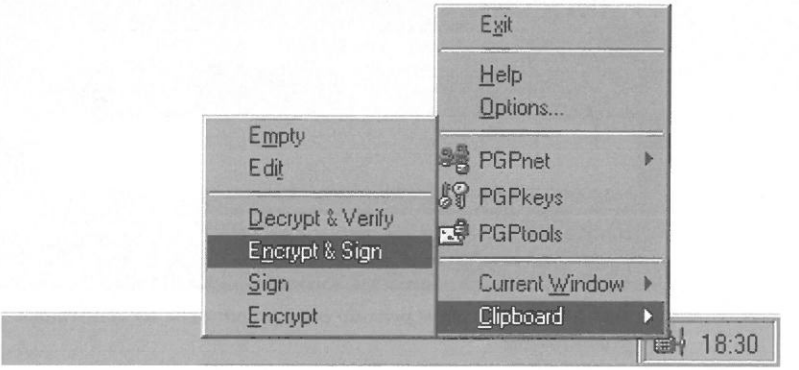
2. Una vez terminado el mensaje y antes de que lo envíe o lo coloque en la cola de envío, vienen los pasos para encriptar. Marque en primer lugar con el mouse el texto real del mensaje.

3. Después abra el menú contextual señalando la marca con el botón derecho del mouse y seleccione aquí el comando *Copiar* o *Copy*. Con esto trasladará el texto del mensaje al Portapapeles.



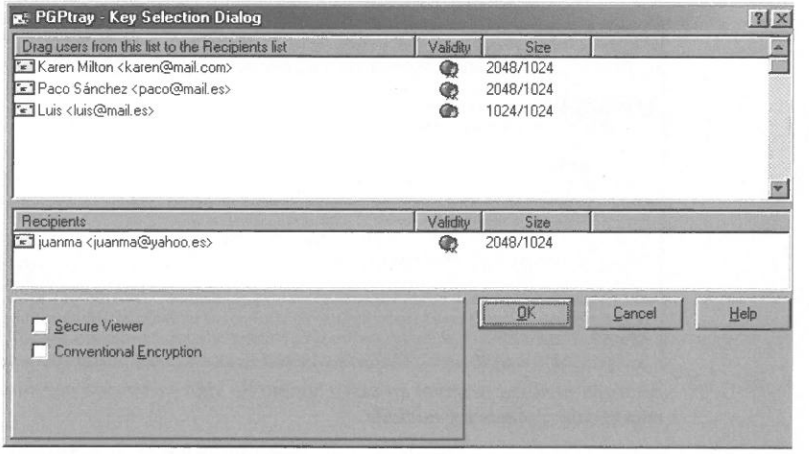
Copie el contenido del mensaje al Portapapeles.

4. Para iniciar la encriptación y firma del mensaje seleccione *Clipboard/Encrypt & Sign* dentro del menú contextual del icono de *PGPTray* de la Bandeja de sistema.



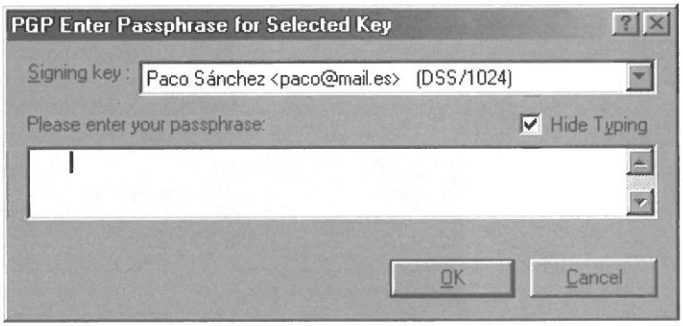
Seleccione en PGPTray la función para encriptar y firmar en el Portapapeles.

5. A continuación elija la clave pública para la que deba ser encriptado el mensaje. Para desplazar una entrada desde la libreta de claves a la lista de destinatarios situada en la parte inferior, arrástrela con el botón del mouse de arriba hacia abajo o haga doble clic en una de las entradas. Una vez seleccionados todos los destinatarios deseados haga clic sobre *OK*.



Elija para quién deba ser encriptado el contenido del Portapapeles.

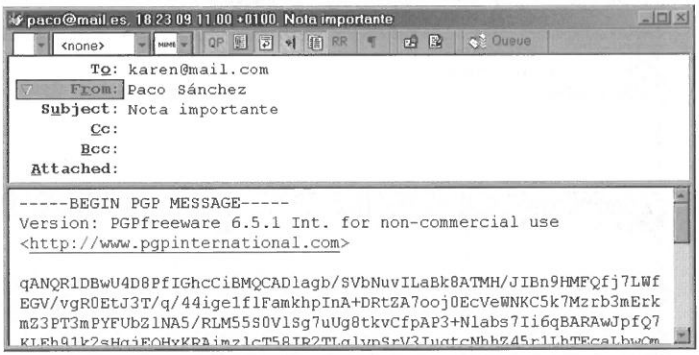
6. Como el mensaje no sólo debe ser encriptado, sino también firmado con la clave privada, deberá introducir a continuación su frase contraseña para autorizar la utilización de la clave privada.



La utilización de la clave privada para firmar debe ser confirmada mediante la frase contraseña.

7. Ahora PGP comenzará la encriptación. En función de la longitud de las diferentes claves esto podrá llevar un rato. Después PGP trasladará el mensaje encriptado al Portapapeles.

8. Vuelva a pasar a su programa de correo electrónico. Sustituya aquí el texto legible original del mensaje por la versión encriptada del Portapapeles. Para ello lo mejor será que vuelva a marcar el texto del mensaje y lo sustituya por el contenido del Portapapeles con *Edit/Paste*.



Ahora el mensaje original en texto legible ha sido sustituido por su versión encriptada y puede ser enviado.

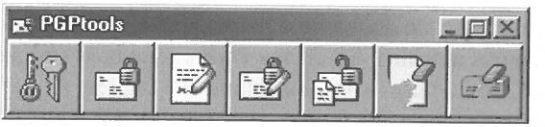
9. Ahora usted puede mandar por el procedimiento habitual el mensaje así encriptado, o colocarlo en una cola de espera para ser enviado.

En el menú contextual del icono *PGPTray*, usted dispone en la Bandeja de sistema de todas las funciones de PGP. A la hora de manejarlo lo importante es que antes haya copiado al Portapapeles el texto que quiera procesar y que, después, vuelva a trasladar los textos desencriptados o encriptados por PGP desde el Portapapeles a la aplicación.

La encriptación de archivos adjuntos

Cada vez goza de mayor popularidad intercambiar por correo electrónico no sólo mensajes sencillos, sino también archivos adjuntos. Al hacerlo hay que tener en cuenta que los archivos adjuntos a un e-mail no son encriptados automáticamente con él. Si también hay que transmitir los archivos en formato confidencial habrá que protegerlos adicionalmente. No se fíe de los procedimientos seudo seguros, como por ejemplo archivos ZIP con protección por palabra clave o documentos Office protegidos por contraseña. Estos métodos no ofrecen ninguna encriptación fiable. Según hemos explicado detalladamente en el Capítulo 2, las contraseñas correspondientes pueden averiguarse con bastante rapidez, si se dispone del software adecuado. En lugar de todo esto, cuando envíe archivos confidenciales también podrá recurrir a PGP. Igual que hace con los mensajes de texto, este sistema también es capaz de encriptar archivos binarios completos, y así protegerlos contra terceros no autorizados.

1. Para poder encriptar un archivo, abra primero con *Inicio/Programas/PGP/PGPTools* o a través del icono de PGP de la Bandeja de sistema, el centro de control de PGP: *PGPTools*.



PGPtools- El centro de control de PGP.

2. Haga clic aquí sobre el botón *Encrypt*.

3. En el siguiente cuadro de diálogo de selección de archivos introduzca el(los) archivo(s) que desee encriptar.
4. A continuación seleccione, como siempre, la clave del destinatario para quien deba ser codificado el archivo e inicie la encriptación.
5. Después encontrará en el índice de salida del archivo a encriptar un nuevo archivo. Llevará el mismo nombre que el archivo de partida, pero con la extensión *.pgp*.

El archivo creado de esta manera y encriptado podrá ser enviado sin problemas por correo electrónico. Estará igual de protegido que el e-mail codificado con PGP. El destinatario sólo deberá tener instalado su programa PGP. Cuando llame al archivo encriptado se abrirá automáticamente la ventana para la introducción de la frase contraseña de PGP. Una vez introducidos los datos correctos el archivo será desencriptado por PGP y restaurado en el ordenador del destinatario.

¿Hasta qué punto es fiable PGP?

En un sistema de encriptación, la fiabilidad siempre se mide por lo fácil que les resulte a personas no autorizadas reventar una clave y convertir en legible un texto cifrado. En los algoritmos usados por PGP la probabilidad de que esto ocurra depende de la longitud de la clave empleada. Con cada bit adicional de longitud de clave se incrementa potencialmente el esfuerzo necesario para descifrarla. En algún momento el esfuerzo requerido para probar todas las posibilidades llega a ser tan grande, que ni siquiera un superordenador moderno sería capaz de calcularlo dentro del lapso vital que esperamos cumpla nuestro universo. Se supone que un algoritmo de encriptación de este tipo puede ser calificado de seguro, aunque resulta imposible demostrar matemáticamente para los algoritmos de encriptación empleados por PGP que no pueda existir alguna puerta trasera. Por tanto, podría ser que los revienta-códigos de la NSA americana hayan encontrado hace tiempo algún método para leer fácilmente los mensajes encriptados con PGP, aunque por otra parte esto no parece demasiado factible. Existen algunos algoritmos conocidos cuya seguridad puede ser demostrada matemáticamente, pero son demasiado complicados para poder emplearlos en la práctica.

Para centrar esta respuesta tan dudosa a la pregunta sobre la fiabilidad: según los conocimientos técnicos actuales, las claves PGP que tengan suficiente longitud (por ejemplo 2048 bits o más) son absolutamente fiables. Al menos sólo las grandes organizaciones estatales como la NSA, o en Alemania la BND, deberían disponer de las posibilidades técnicas para reventar el encriptamiento (si es que las tienen). Pero en cualquier caso no es muy recomendable meterse con ellas, aunque sea usando PGP. Lo importante es que el vecino, el jefe o el compañero de trabajo malévolo, no pueden reventar el PGP.

Aquí lo más importante es que usted guarde su clave privada como la niña de sus ojos. Si alguien le espía mientras introduce la contraseña y después tiene acceso a su PC para copiarse su archivo de claves, todo esto de la encriptación tendrá poco sentido. Si usted sospecha en algún momento que haya podido ocurrir algo así, cree inmediatamente una nueva clave y pida a su compañero de comunicación que dejen de utilizar la vieja inmediatamente.

S/MIME – la alternativa de pago

Como alternativa a PGP existe actualmente un sistema de encriptación comercial basado en S/MIME (***Secure Multipurpose Internet Mail Extension***), que también trabaja con claves asimétricas llamadas aquí certificados. Programas de correo electrónico populares como Outlook Express y Netscape Messenger soportan de origen este sistema, sin necesidad de plug-in especiales. En principio los certificados S/MIME son absolutamente equiparables a las claves PGP, aunque tienen algunas desventajas importantes:

- En comparación con PGP, los certificados son mucho más inseguros. Como el software ha sido desarrollado por Microsoft en los Estados Unidos, está sujeto a las restricciones vigentes allí para la exportación de armas (en los Estados Unidos, la encriptación entra como tecnología militar en el apartado de las armas). Por esta razón, con las versiones internacionales de este software sólo se pueden emplear claves hasta ciertos limites, no precisamente calificables de insuperables. PGP permite crear claves mucho más grandes, que prácticamente son consideradas como inexpugnables.
- Mientras en PGP los usuarios se crean sus propias claves, los certificados son concedidos por una entidad certificadora central. Aquí el usuario no puede controlar quién podría recibir copia de su certificado personal.
- Además, estas entidades no son organizaciones de interés público, sino empresas de servicios que buscan beneficios, es decir, que el usuario deberá pagar los certificados, mientras las claves PGP son absolutamente gratuitas.

Consiga su propio certificado

Antes de poder encriptar o firmar mensajes con S/MIME usted necesita, en primer lugar, su propio certificado. En contraste con PGP aquí no lo puede generar usted mismo. Deberá solicitarlo a una entidad certificadora, cosa que por desgracia no está exenta de costes. Pero para una primera prueba, al menos, puede conseguir un certificado de test gratuito. Por ejemplo, el proveedor *VeriSign* (http://www.verisign.com) proporciona certificados de prueba gratuitos por 60 días. Para obtener un certificado propio hay que dar los siguientes pasos:

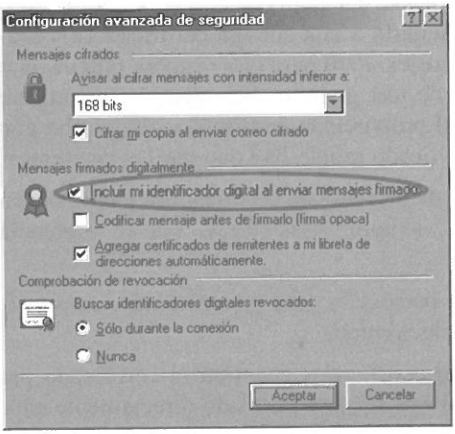
1. Visite la página web de una entidad certificadora y elija un certificado propio. Suele haber casi siempre varias ofertas, que se diferencian por el precio y las prestaciones.
2. Introduzca los datos personales para el certificado, como su nombre y su dirección de correo electrónico.
3. Ahora el servidor de certificados generará el certificado para usted. Por razones de seguridad éste no será instalado directamente en su navegador. Primero le enviarán un código a la dirección de correo electrónico que usted indicara. Con esto pretenden garantizar que nadie pueda generar certificados para direcciones de correo electrónico que no le pertenezcan.
4. Una vez recibida la notificación por e-mail (esto suele tardar sólo unos pocos minutos), vuelva a la página web de la entidad certificadora e introduzca allí el código, con el que podrá instalar su certificado.
5. El certificado es instalado automáticamente en el programa de correo electrónico y usted podrá disponer de él desde ese mismo momento.

No se preocupe si a primera vista todo esto le suena demasiado complicado. Casi siempre las páginas web de las entidades certificadoras incluyen un asistente, que le guiará a usted rápidamente por los pasos necesarios.

Distribuir los certificados S/MIME

De modo similar a las claves públicas de PGP, también los certificados tienen una parte pública. Es la que necesita el remitente de un mensaje encriptado para podérselo codificar a usted. Si quiere distribuir su certificado a otros deje que Outlook Express lo adjunte automáticamente a todos los mensajes que contengan la firma digital de usted.

1. En Outlook Express, abra con *Herramientas/Opciones...* el cuadro de diálogo *Opciones* y pase a la pestaña *Seguridad.*
2. Haga clic sobre el botón *Avanzadas...* para abrir la *Configuración avanzada de seguridad.*
3. Active en el apartado *Mensajes firmados digitalmente* la opción *Incluir mi identificador digital al enviar mensajes firmados.*
4. Confirme la nueva configuración con doble *Aceptar.*



Haga que su certificado sea publicado automáticamente.

A partir de ahora, siempre que envíe mensajes con una firma digital estos contendrán también la parte pública de su certificado, que permitirá al destinatario verificar la autenticidad del mensaje. Si un compañero de comunicación necesita la parte pública del certificado de usted para mandarle un mensaje confidencial, sólo será necesario que le envíe un mensaje con firma digital. En este van incluidos todos los datos necesarios.

Encriptar y firmar certificados S/MIME

La creación de mensajes encriptados o e-mail con certificados se desarrolla de modo muy parecido a PGP. Estas funciones están totalmente integradas en las de redacción de un e-mail en Outlook Express y sólo requieren uno o dos clics adicionales del mouse.

- Si quiere encriptar un mensaje para el destinatario haga clic en algún momento de la redacción, pero como muy tarde justo antes del envío, sobre el botón Cifrar. Cuando realice el envío Outlook Express creará automáticamente un mensaje encriptado a partir del texto original. La condición indispensable para esto es que la parte pública del certificado del destinatario esté almacenada en su libreta de direcciones, es decir, que usted ya haya recibido una vez un mensaje con esta parte pública. De lo contrario Outlook Express se quejará con un mensaje de error.

- Para firmar un mensaje haga clic sobre el botón *Sign (S/MIME)*. Antes de enviarlo Outlook Express le pondrá su firma digital, por la que los destinatarios podrán reconocer la autenticidad del e-mail.

Desencriptar mensajes que lleven certificados S/MIME

En realidad no hace ninguna falta desencriptar los mensajes que fueran encriptados para usted o firmados digitalmente, ya que en gran medida Outlook Express se encarga de esta tarea automáticamente. Así, en los mensajes que vayan firmados digitalmente, estas firmas son comparadas con los certificados almacenados. Si se detectan diferencias o si usted no posee el certificado del remitente, Outlook Express se lo advertirá inmediatamente. También la desencriptación de mensajes se realiza de modo automático. Así, usted ve enseguida la versión de un e-mail en texto legible descodificado.

7.4 Ocultar en lugar de desencriptar – protección mediante esteganografía

La encriptación de mensajes aplicando los métodos de la criptografía es un medio eficaz para garantizar comunicaciones seguras. Desgraciadamente muchos gobiernos ven en esta técnica un peligro. A fin de cuentas no sólo ofrece posibilidades de protección a ciudadanos honestos y conscientes de la seguridad. También criminales o terroristas podrían emplear las técnicas de encriptación para concretar sus crímenes sin que nadie les moleste. Del mismo modo se pueden transportar, encriptados, contenidos ilegales. Al menos, estos son los

argumentos esgrimidos por políticos y servicios de información para exigir una regulación legal (y con ello, la restricción) de la criptografía. Como siempre, los Estados Unidos van muy por delante. Con el desarrollo del Clipper-Chip el gobierno ha insertado en la criptografía una puerta trasera para sus servicios secretos.

INFO

¿Qué es el Clipper-Chip?

El Clipper-Chip es un encriptador por hardware de nuevo desarrollo. Emplea diferentes métodos de cifrado seguros y, en el futuro, se pretende que sea aplicado en todos los ámbitos de las transacciones on-line. La característica decisiva del chip es que lleva incorporada una puerta trasera. Si bien los usuarios reciben una clave propia muy difícil de violar por los métodos tradicionales, los servicios secretos americanos, como la National Security Agency, poseen una "clave general" que permite descifrar cualquier mensaje Clipper. Las desventajas de esta técnica saltan a la vista: con ella las autoridades estatales pueden vigilar en todo momento la comunicación entre sus ciudadanos. Aunque existan límites legales concisos para este tipo de medidas de escucha, ningún ciudadano puede controlar si estas normas son respetadas o no. Y los servicios secretos americanos no son precisamente famosos por su fidelidad a las leyes. Otra pregunta que surge es si la clave general no pudiese acabar en manos de quien no debe. Un empresario que pueda espiar a sus competidores, confiados en la supuesta seguridad de la encriptación Clipper, podría obtener incalculables ventajas sobre la competencia. También en Alemania crece el clamor por una regulación de este tipo, y aunque el Ministerio del Interior haya fracasado varias veces con iniciativas legales al respecto, seguramente sólo será cuestión de tiempo que éstas se impongan.

La idea: ocultar información confidencial entre masas de datos

En el futuro ¿cómo podremos seguir protegiendo individualmente nuestra comunicación, pese a las estrictas regulaciones de la criptografía? En principio tenemos la posibilidad de hacer caso omiso de las regulaciones y seguir empleando procedimientos de encriptación seguros y no sujetos a controles. Pero una vez aprobadas las leyes pertinentes esto podría pasar a ser un delito, por lo que no resulta recomendable, especialmente, porque los mensajes cifrados pueden ser reconocidos fácilmente por su aparente falta de sentido.

Una solución al problema la propone la ciencia de la ocultación, la esteganografía. Ésta se ocupa de ocultar información importante dentro de otro tipo de informaciones, de manera que no se le ocurra a nadie buscarla allí. Cómo funciona esto, puede ser explicado por un ejemplo sencillo. Supongamos que un amigo le envía a usted una postal desde su lugar de vacaciones:

¡Un saludo desde Nueva York! ¡Todo es maravilloso!

A primera vista, parece algo muy normal. Pero sigamos suponiendo que antes de partir su amigo, usted acordara con él un método para que le pudiera hacer llegar información secreta. El método consiste en redactar el texto de la postal de tal forma, que cada 10º carácter (sin incluir los espacios en blanco) sea parte de un mensaje secreto. Entonces, el texto de arriba debería leerse como sigue:

¡Un Saludo deSde Nueva YOrk! ¡Todo eS maravilloso!

Visto así, distinguimos como misiva secreta la llamada internacional de socorro *SOS*. Quien no conozca el método acordado sólo apreciaría el contenido obvio y jamás pensaría que detrás pueda ocultarse un mensaje totalmente diferente.

INFO

La gestación de la esteganografía

Igual que la criptografía, la esteganografía no es ningún invento nuevo de la era informática. Sus raíces se remontan, como mínimo, a la antigua Grecia. En esos tiempos aún se empleaban métodos bastante drásticos. El historiador Herodoto habla de un noble que hizo rapar a sus esclavos para tatuarles en el cuero cabelludo mensajes secretos. Cuando les había vuelto a crecer el pelo enviaba a los esclavos de camino. Llegados a su destino les volvían a cortar la cabellera, con lo que el mensaje quedaba a la vista. Y es que en aquella época la gente todavía disponía de mucho tiempo. Posteriormente, sobre todo los servicios secretos fueron inventando constantemente nuevos métodos de esteganografía. Los agentes alemanes emplearon durante la Segunda Guerra Mundial los Microdots, unos microfilms diminutos y esféricos ya impresionados, que eran pegados en cartas normales como puntos de las íes. Estos microfilms podían contener varios folios mecanografiados, pero también planos técnicos o fotografías.

Esteganografía informatizada

Con la esteganografía informatizada se ha desarrollado un apartado totalmente nuevo de esta ciencia. Con sus gigantescas masas de datos los ordenadores ofrecen muchos escondites para la información secreta. Los ejercicios estándares incluyen esconder mensajes de texto en archivos digitales de imagen o sonido. Para ello se aprovecha el almacenamiento binario y se trabaja con el efecto de ruido de fondo. Para almacenar digitalmente informaciones gráficas o acústicas éstas son fraccionadas en bits, es decir, en las unidades de información menores de 1 y 0. Para un punto de matriz o la breve fracción de una grabación sonora, se emplea siempre un mínimo de 1 byte (compuesto de 8 bits). Si ahora se modifica uno de esos ocho bits también quedará falseada la información contenida en él. Sin embargo, seleccionando cuidadosamente los bits manipulados este cambio no es perceptible por el ojo o el oído humano, por caer ya en el campo de lo que se llama murmullo de fondo.

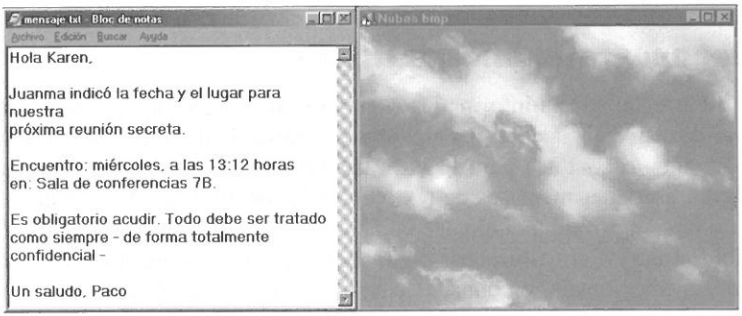
Del hecho de que por cada byte de datos sólo se pueda ocultar 1 bit de información, se desprende que la masa de datos siempre debe ser mucho más grande que la cantidad de información a ocultar.

¿Hasta qué punto es segura la esteganografía?

La esteganografía en sí es poco segura. Si alguien conoce el procedimiento aplicado y los datos con el mensaje oculto, podrá recuperar la información sin problemas. Los procedimientos esteganográficos no emplean ninguna clave como la criptografía clásica. La esteganografía apuesta totalmente por el efecto de la ocultación. Los datos de camuflaje son seleccionados de tal modo, que nadie piense jamás que puedan contener misivas secretas. Por lo que nadie intenta desencriptar los datos. Para ir realmente a lo seguro habría que combinar la esteganografía con los procedimientos de encriptación. Primero se codifican criptográficamente los mensajes confidenciales. Después, aplicando la esteganografía se oculta el texto de la clave en datos inofensivos. Aunque ahora alguien descubriera la información escondida, además tendría que ser capaz de desencriptarla.

Ocultar misivas secretas en imágenes

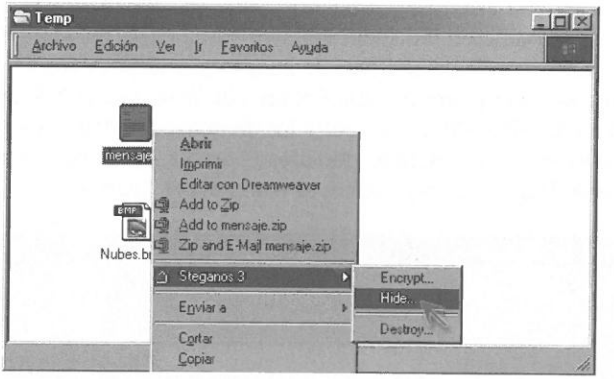
En este apartado queremos mostrarle cómo funciona el software de esteganografía recurriendo a un ejemplo práctico. Vamos a utilizar para ello el software *Steganos Security Suite* para Windows. Usted mismo puede descargar de Internet una versión de evaluación gratuita de este programa en http:// www.steganos.com. Éste es capaz de ocultar cualquier archivo dentro de archivos de imagen, sonido o texto. Aparte de eso, Steganos Security Suite ofrece una amplia gama de funciones relacionadas con la encriptación y la seguridad. Aunque en este apartado nos vamos a limitar a ocultar un texto breve dentro de un archivo de gráficos.



El texto de la izquierda debe esconderse discretamente en la imagen de la derecha.

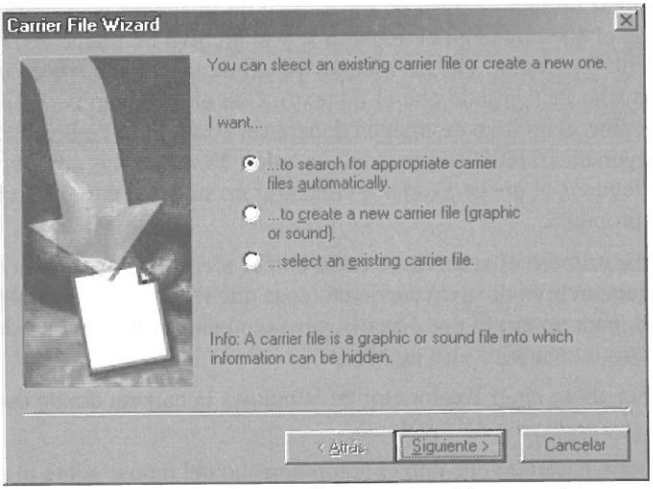
Para ocultar un texto dentro de un archivo de imágenes necesitará siempre dos archivos: el que contenga el texto en sí y el archivo de imágenes, llamado también archivo portador. Por las razones ya expuestas, el archivo de imagen deberá ser mucho más grande que el de texto. Con una imagen de 8 bits de intensidad de color, el archivo de imagen deberá ser como mínimo 8 veces mayor. Con una imagen de 16 bits de intensidad de color, 16 veces más grande, etc. No obstante, Steganos le puede ayudar a encontrar en su disco duro el archivo de imágenes apropiado.

1. Cree primero el archivo de texto con el mensaje que quiera ocultar. Podrá ser un archivo de texto corriente (cosa que resulta recomendable, por ejemplo, para un envío por e-mail), pero también un documento de proceso de textos o cualquier otro archivo.
2. Abra ahora en el Explorador de Windows la carpeta donde esté almacenado ese archivo y márquelo allí.
3. Ahora, haciendo clic con el botón derecho del mouse sobre el archivo, abra el menú contextual. Aquí encontrará desde la instalación de *Steganos 3* Security Suite la opción Steganos 3 más el submenú, donde deberá seleccionar *Steganos 3/Hide.*



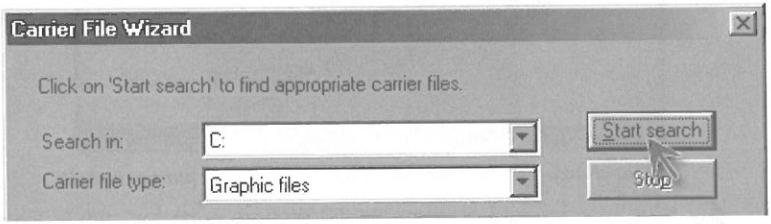
Elija el archivo que contiene el mensaje secreto, para ocultarlo.

4. Con esto iniciará el asistente del archivo portador, que le ayudará a elegir el archivo donde deba ser escondido el mensaje. Con él podrá elegir uno de los archivos portadores existentes (*...select an existing carrier file*), ordenar la búsqueda automática de los archivos portadores apropiados (*...to search for appropiate carrier files automatically*) o crear un nuevo archivo portador -gráfico o sonido- (*...to create a new carrier file –graphic or sound-*). Si usted no tiene ya pensado un archivo concreto como portador, la opción *...to search for appropiate carrier files automatically* le ayudará a trabajar más deprisa.



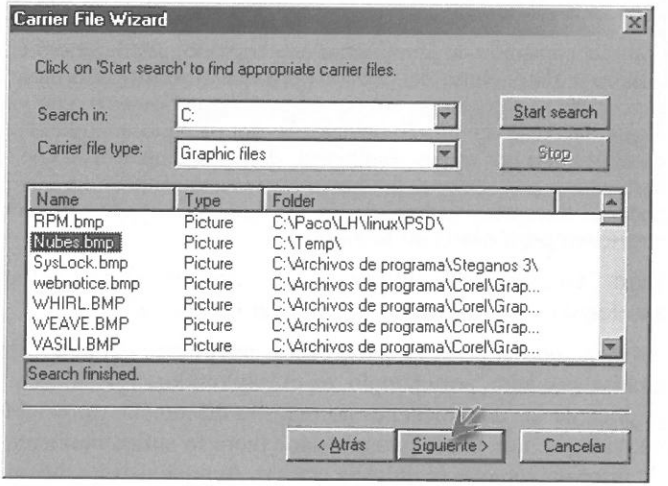
Decida de dónde deberá tomar Steganos el archivo portador requerido.

5. Ahora se iniciará una función de búsqueda en la que Steganos analizará los archivos existentes en su disco duro y propondrá los archivos portadores apropiados. Así usted no necesita ocuparse personalmente de la búsqueda. Aunque es condición indispensable que posea en su PC una selección suficientemente grande de archivos de imagen y sonido. Antes de que se inicie la búsqueda, aún podrá delimitar el área de búsqueda con *Search in:* (buscar en:) a un disco duro concreto y los archivos que deban ser analizados, a un tipo concreto de archivo portador (*Carrier file type*), para acelerar la búsqueda. Haga clic ahora sobre el botón *Start Search*.



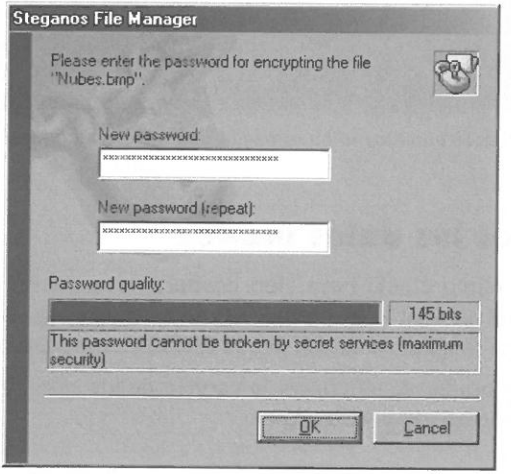
Haga que sus discos duros sean explorados automáticamente en busca de los archivos portadores apropiados.

6. El asistente del archivo portador de Steganos explorará el disco duro especificado en busca de los archivos apropiados y creará una lista. Si ésta es ya suficientemente larga, usted puede interrumpir el proceso de búsqueda en cualquier momento haciendo clic sobre *Stop*. Para seleccionar como archivo portador uno de los visualizados marque la entrada correspondiente y haga clic sobre *Siguiente*. Confirme después la selección con *Finalizar* o *Finish*.



Elija un archivo portador en la lista de los archivos disponibles.

7. También cuando se oculta en un archivo portador se encripta la información secreta por razones de seguridad. De lo contrario, cualquier otro usuario de Steganos podría reconstruir los mensajes. Por eso introduzca en el siguiente paso una contraseña, a partir de la cual Steganos calculará una clave simétrica. Para que el destinatario del archivo pueda reconstruir el mensaje oculto, usted deberá comunicarle la contraseña por una vía independiente. Memorice bien esa contraseña. Si la olvida o la extravía se perderán los datos ocultos. Según declaraciones del fabricante de Steganos, ni él mismo posee una puerta trasera que pueda ayudar en estos casos.



Introduzca una contraseña para encriptar la información secreta.

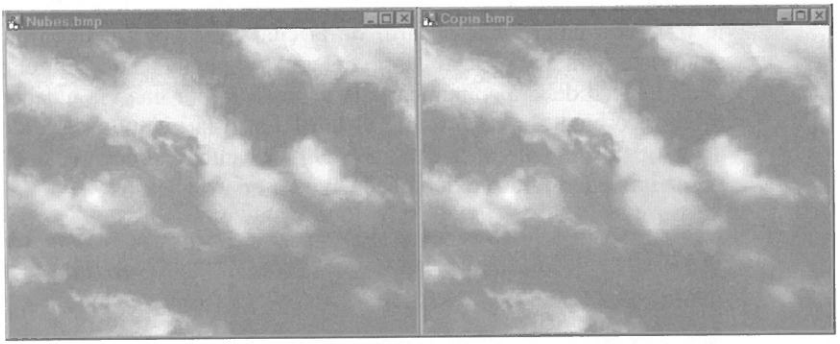
TRUCO

Envío de la contraseña

Como el contenido de la misiva está encriptado, usted deberá enviar la contraseña al destinatario del archivo para que él pueda reconstruir el texto. Es importante que para esta entrega elija, obligatoriamente, una vía independiente del envío del propio archivo. Si, por ejemplo, manda el archivo esteganografiado por correo electrónico, debería comunicar la contraseña al destinatario por teléfono. Si la anotara sencillamente en un e-mail, cualquiera podría interceptar ese mensaje, con lo que ya dispondría de todos los medios necesarios para averiguar la misiva secreta.

8. Ahora Steganos ocultará los datos discretamente dentro del archivo portador elegido y lo almacenará en su lugar de origen.

Una vez concluido el proceso usted puede cerciorarse del resultado visualizando el archivo portador, por ejemplo, en el Explorador de Windows. Una comparación óptica de las dos imágenes no muestra diferencias apreciables por el ojo humano, siempre que el archivo portador fuera lo suficientemente grande para alojar la información que se quisiera ocultar. Aunque usted eche un vistazo a las propiedades detalladas del nuevo archivo, no apreciará diferencias con respecto al archivo de partida. El tamaño es el mismo hasta el último byte. Sólo la fecha del archivo revela que fue modificado recientemente.



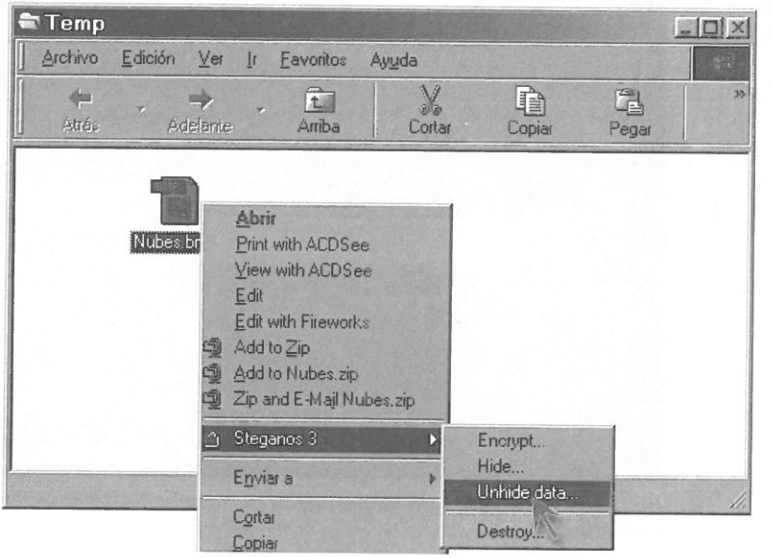
En una de estas imágenes (izquierda) se ha ocultado una misiva secreta. ¿Vé alguna diferencia?

Volver visibles los datos ocultos

Si usted tiene un archivo donde haya sido ocultada información secreta con Steganos, la podrá volver visible empleando el mismo programa. La única condición es que conozca la contraseña con la que fueran encriptados los datos.

1. Abra en el Explorador de Windows la carpeta donde esté almacenado el archivo esteganografiado y selecciónelo.

2. Ahora haga clic con el botón derecho del mouse sobre el archivo y, en el menú contextual, seleccione *Steganos 3/Unhide data*.



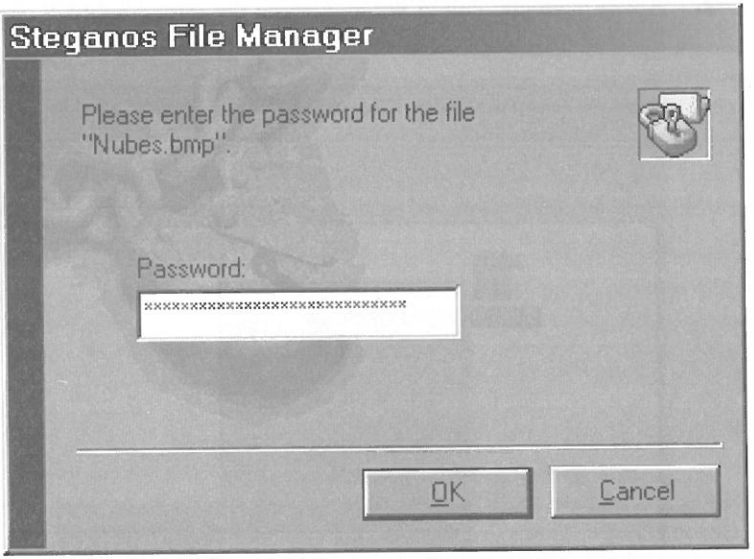
Elija la función de Steganos para restaurar los datos ocultos.

TRUCO

¿No está disponible la función para restaurar los datos?

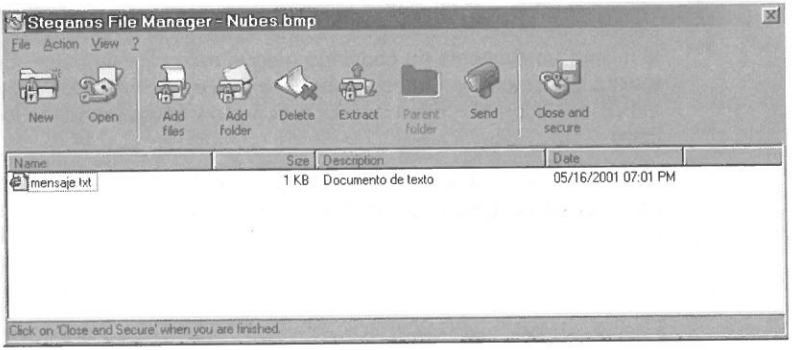
Si en el menú contextual no aparece la función *Unhide data* se deberá a que Steganos no puede encontrar datos ocultos en el archivo seleccionado. Es posible que usted haya elegido accidentalmente el archivo equivocado, o que el mismo simplemente no contenga ningún escondite de datos. En última instancia, quizá también pueda deberse a que el archivo – tal vez al ser transmitido por Internet – haya quedado dañado y Steganos ya no lo pueda analizar.

3. Ahora Steganos pide la contraseña para poder desencriptar los datos ocultos. Sin ella es imposible hacer esa recuperación.



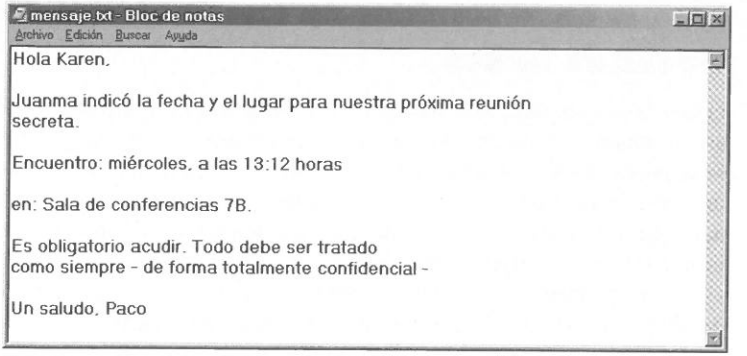
Indique la contraseña, con la que fueran encriptados los datos secretos antes de su ocultación.

4. Steganos reconstruye ahora los datos y los desencripta. A continuación abre su propio gestor de archivos Steganos (*Steganos File Manager*), donde será visualizado el contenido del archivo portador. Aquí encontrará usted los datos ocultos.



En el gestor de archivos Steganos se visualiza el contenido secreto de los archivos portadores.

5. Haciendo doble clic puede abrir y visualizar los archivos señalados.



Los datos ocultos están desencriptados.

6. Para poder almacenar como archivo independiente los datos que fueran ocultados en un archivo portador, elija la opción *Action/Extract*. Con ella podrá exportar a cualquier carpeta los archivos desencriptados.

7.5 Freemailer – gratuitos, pero no exentos de peligro

Un nuevo servicio que se ha abierto camino muy deprisa en Internet son los llamados freemailer, los proveedores de correo electrónico gratuito. Estos facilitan al usuario de Internet gratuitamente direcciones y buzones de e-mail. Así se puede disponer de correo electrónico sin depender de proveedores de servicios on-line, ni de un proveedor de Internet. Pero, ¿cómo está la seguridad en los accesos de e-mail a través de la Red? Nosotros vamos a revelarle con qué deberá tener cuidado y cómo puede sacar provecho de los freemailer con seguridad.

INFO

Hackers hacen de las suyas en GMX

En el verano del 2000 el popular freemailer GMX fue víctima del ataque de hackers. Mediante un virus que se activaba automáticamente al abrir un mensaje, los malhechores pudieron manipular la contraseña de los usuarios de GMX. Según la versión oficial de la empresa, las contraseñas de 1625 usuarios "sólo" fueron borradas, pero no espiadas. El suceso no fue el único de este tipo. También otros freemailer han sido y siguen siendo víctimas de ataques y agujeros de seguridad. Los freemailer ejercen tanto atractivo sobre los hackers, porque son sistemas abiertos y cualquiera puede hacerse miembro sin más requisitos cuando le plazca, de modo que el siguiente ataque prácticamente puede lanzarse desde dentro. Además, los freemailer suelen tener un gran número de usuarios, por lo que un virus infiltrado o un troyano instalado, en muy poco tiempo podría afectar a muchos miles de usuarios, y aunque un ataque sea detectado pronto, el esfuerzo casi siempre habría valido la pena.

Más información sobre el pirateo a GMX:
http://www.zdnet.de/news/artikel/2000/07/19011-wc.html

GMX & Co. – servicios de correo electrónico a través de la Red

Quien posee un acceso a Internet, en la mayoría de los casos también dispone automáticamente de una dirección de correo electrónico. Si, por ejemplo, usted se conecta telefónicamente a través de un proveedor de Internet o es cliente de un servicio on-line, la dirección de correo electrónico viene incluida de forma natural en la tarifa base mensual. Desgraciadamente, si alguien renuncia voluntariamente a utilizar el correo electrónico los proveedores no rebajan parte de la tarifa. Y entonces, ¿para qué se necesita otra dirección – aunque sea gratuita – de correo electrónico? En principio, una dirección independiente del proveedor de Internet o del servicio on-line puede ser de gran utilidad: precisamente en esos servicios on-line, con frecuencia el buzón de correo es literalmente inundado de mensajes publicitarios. Si, por el contrario, usted utiliza otra dirección de correo electrónico, estará bien protegido contra esta clase de agobios.

Además, ¿quién dice que usted va a seguir siendo toda la vida cliente de su actual proveedor? Normalmente cada cambio de proveedor traería consigo el cambio de su dirección de correo electrónico, con lo que tendría que comunicársela otra vez a todos sus conocidos y amigos. Cuando la dirección se emplea para los negocios, estos cambios de todos modos no pueden hacerse. Si usted tiene una dirección independiente del proveedor o del servicio on-line podrá cambiar tantas veces como quiera. Además, frecuentemente las direcciones de correo electrónico gratuitas ofrecen funciones especiales relacionadas con el e-mail, que son impensables en su proveedor de Internet o su servicio on-line. Como, por ejemplo, las funciones autoreply, que le permiten contestar automáticamente a los remitentes de mensajes, si usted no puede o no quiere leer su correo electrónico durante un tiempo prolongado. También es muy práctica la posibilidad de remitir a un móvil los mensajes que entren. Así, si ha recibido un mensaje importante usted se enterará enseguida.

Además, hace tiempo que para acceder a Internet, ya no hace falta darse de alta en un servicio on-line o un proveedor de Internet desembolsando la correspondiente tarifa base. Los accesos call-by-call permiten conectarse telefónicamente de un modo flexible y sin ningún tipo de problemas. Aunque también en estos casos se necesita una dirección fija de correo electrónico para poder ser localizado.

INFO

¿Servicios secretos como proveedores de correo electrónico?

Durante mucho tiempo la pregunta por la financiación de los proveedores de correo electrónico gratuito encendió los ánimos. Una teoría que se ha mantenido hasta hoy con obstinación es la siguiente: los operadores de estas ofertas serían en realidad los servicios secretos, que quieren controlar así el tráfico de correo electrónico. A fin de cuentas, de esta manera podrían comprobar cada e-mail que pase por su servidor. ¿Será verdad? Naturalmente, los proveedores de correo electrónico lo niegan categóricamente. Pero, ¿qué otra

cosa se puede esperar? Queda el hecho de que los servicios secretos disponen en abundancia de otras posibilidades para controlar el correo electrónico. Además, de un modo u otro, siempre podemos encriptar nuestros e-mail para evitar que los lean personas a las que no van destinados, según hemos explicado ya en detalle.

Relación de los proveedores más importantes

Para que usted no tenga perder tiempo buscando por ahí y probando qué proveedor es el mejor, le hemos recopilado los más importantes. Todos estos proveedores facilitan direcciones de correo electrónico gratuitas. En la mayoría de los casos, para utilizarlas hay que recurrir a una interfaz web que sólo necesita un navegador web cualquiera. Estas interfaces suelen tener un diseño muy funcional y basta un breve periodo de adaptación para manejarlas bien. Además, algunos servicios también ofrecen la posibilidad de remitir automáticamente los mensajes recibidos a otra dirección de correo electrónico (por ejemplo, la que usted tenga de su proveedor de Internet o de los servicios on-line). A la inversa funciona el servicio de recogida POP3, donde el servidor del proveedor puede recoger automáticamente los mensajes de otros buzones de correo POP3. Esto es muy práctico para los usuarios que posean varias direcciones.

Proveedor	Dirección	Direcciones de correo electrónico
Terra	http://www.terra.es	<Name>@terra.es
GMX	http://www.gmx.com	<Name>@gmx.de <Name>@gmx.net <Name>@gmx.com
Hotmail	http://www.hotmail.es	<Name>@hotmail.com
Topmail	http://www.topmail.com	<Name>@topmail.com
Lycos	http://www.lycos.es	<Name>@lycosmail.com <Name>@iname.com <Name>@cyberdude.com <Name>@cybergal.com <Name>@technologist.com
Yahoo	http://www.yahoo.es	<Name>@yahoo.es

TRUCO

Correo electrónico gratuito con servidor POP3 propio

La mayoría de proveedores de direcciones gratuitas de correo electrónico trabajan a través de la Red, es decir, los mensajes recibidos pueden ser remitidos a otra dirección de correo electrónico, o leídos directamente desde un servidor web. Pero algunos servicios, como por ejemplo *GMX* o *Yahoo*, ofrecen también sus propios servidores POP3, de los que se pueden descargar mensajes con cualquier programa de correo electrónico. También disponen

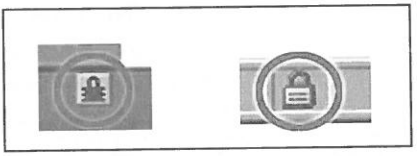
de un servidor STMP para enviar los mensajes. En este caso la utilización no es diferente de la de un apartado de correo en un servicio on-line o un proveedor de Internet.

Más vale prevenir – las reglas más importantes a seguir con los servicios de freemail

Y ahora ¿cómo está el asunto de la seguridad cuando se emplean servicios de freemail? Desgraciadamente, en líneas generales hay que decir que la lectura y escritura de e-mail a través de una interfaz basada en la Red, es menos segura que emplear un programa de correo electrónico que comunique directamente con servidores de correo entrante y saliente. La causa reside, sobre todo, en el navegador web que sirve de interfaz para el editor de mensajes. Los navegadores web tienen gran cantidad de agujeros de seguridad y puntos potenciales de ataque, según hemos expuesto detalladamente en el Capítulo 3. Ahora, de pronto todos estos peligros potenciales también son aplicables a los e-mail escritos y a los recibidos. Por eso es importante que se apliquen una serie de reglas de seguridad.

Conexiones seguras

Verifique siempre si su proveedor de freemail ofrece unas conexiones seguras para la navegación. Esto lo verá rápidamente por el icono del candado visualizado en la Barra de estado de su navegador web. Ya el inicio de sesión debería producirse a través de una conexión segura, para no poner en peligro el nombre del usuario ni la contraseña. Después debería seguir en marcha la conexión segura hasta que usted finalice la sesión. Lo mejor es que no sólo controle la seguridad de la conexión cuando haga logon por primera vez, sino siempre que entre. Es posible que, en caso de caída temporal de un servidor seguro, le trasladen a usted sin que se dé cuenta a un servidor sin medidas de seguridad.

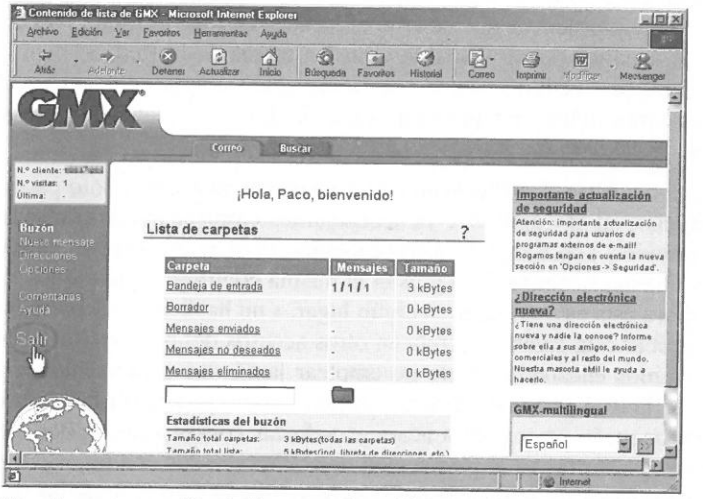


El icono del candado que indica las conexiones seguras en Netscape Navigator (izquierda) e Internet Explorer (derecha).

No olvide cerrar la sesión

Muy importante: cierre la sesión expresamente cada vez que termine de trabajar con el correo electrónico. Aunque lo más natural sea llamar en el navegador web la dirección de otro sitio web, esto es muy peligroso. La mayoría de servicios de correo electrónico a través de la Red trabajan con un *sessionkey*, que libera el acceso a su buzón de correo cuando usted hace logon. Esta clave permanece activa hasta que usted finalice la sesión con su buzón. Si no cierra la sesión este

acceso quedará abierto. Si ahora alguien hubiera espiado su clave, o simplemente la hubiera adivinado a la buena de Dios, podría acceder a su buzón de correo y leer sus mensajes, o incluso redactar e-mail nuevos con su nombre. Es cierto que, en la mayoría de los casos, un mecanismo de seguridad se encarga de que una sessionkey sea anulada tras determinado tiempo sin ninguna nueva acción del usuario, pero en algunos casos estos plazos son de 20 minutos o más, con lo cual dejarían tiempo de sobra al atacante. Basta un simple clic sobre el botón de *Salir* o *Logout*, para erradicar este peligro completamente.



Muy importante: ¡No olvide cerrar la sesión después de haber leído los e-mails!

Fuente de riesgos: los datos históricos

En capítulos precedentes nos hemos ocupado exhaustivamente del peligro que suponen los datos históricos que almacena el navegador web en el PC local a lo largo de una sesión de navegación. Esto también es aplicable a los servicios de correo electrónico a través de la Red, que usted visita desde el navegador web. Si, por ejemplo, usted emplea el PC de la oficina para descargar de un proveedor a través de Red sus e-mail privados, o quizá si desea comprobar rápidamente desde un cibercafé si tiene mensajes nuevos, en el ordenador utilizado quedarán huellas con las que podrían toparse otros, ya sea por casualidad o con intención. Según como funcionen las ofertas de correo electrónico de la Red, los mensajes que usted hubiera descargado anteriormente podrían estar disponibles offline y bastaría con llamarlos desde la barra de historial. Igualmente, los datos de acceso podrían estar desprotegidos y al alcance de todos. En el peor de los casos, con un simple clic en el botón *Atrás* un intruso podría acceder plenamente a sus carpetas de correo (aunque esto sólo ocurriría con ofertas técnicamente muy mal implementadas).

Por lo tanto, si usted tramita sus correos electrónicos desde un PC al que también tengan acceso otros, debería preocuparse de que no queden huellas tras la lectura o escritura de mensajes confidenciales. En el capítulo precedente ya hemos presentado con más detalle las posibles soluciones para esto.

Proteger las contraseñas

En el pasado ha quedado patente muchas veces que las ofertas a través de la Red no siempre garantizan la seguridad de los datos personales. Ya se produjeron repetidamente problemas, que dejaron al alcance de todo el mundo las contraseñas de los usuarios de servicios de e-mail a través de la Red. Si bien hay que decir que los proveedores suelen reaccionar casi siempre con rapidez, desactivando las contraseñas para que ya no sean válidas y el usuario las deba sustituir por otras.

Pero, ¿qué ocurriría si no habíamos empleado esa contraseña sólo para ese servicio? Bueno, en el Capítulo 2 ya aconsejamos emplear la contraseña una sola vez, para evitar precisamente este problema. Pero la realidad es que muchos usuarios eligen el camino fácil y usan la misma contraseña para todos los accesos. Si ahora ésta es publicada en algún lugar, a un hacker se le podría ocurrir la idea de probar esta palabra secreta en otros accesos del mismo usuario. Por eso recomendamos encarecidamente no emplear jamás las contraseñas de accesos basados en la Red para otros ámbitos críticos, como podría ser la banca on-line. Si no, un pequeño error podría acarrear nefastas consecuencias. Por cierto, los operadores de ofertas en la Red suelen dejar claro en sus condiciones generales que en estos casos no se responsabilizan bajo ningún concepto de los daños originados.

Una dirección para cada asunto – aprovechar las direcciones gratuitas de correo electrónico

Ya hemos descrito en el apartado precedente con qué debería usted tener cuidado cuando use direcciones de correo electrónico gratuitas, para que sean tan seguras como las convencionales. Ahora también queremos exponerle cómo emplear estas direcciones gratuitas adicionales, para tramitar su comunicación por correo electrónico con menos problemas y más seguridad. La idea básica es usar una dirección de e-mail diferente para cada asunto. Esto ofrece la ventaja de que, así, podemos decidir siempre qué dirección arriesgamos y dejamos expuesta a ataques de hackers, bombas de e-mails o, simplemente, a que abusen de ella para enviarnos molestos e-mails publicitarios. A continuación vamos a proponer una distribución de las direcciones de correo electrónico para los asuntos más importantes y también le demostraremos las ventajas que ello trae consigo.

Direcciones de correo electrónico estables para asuntos privados y profesionales

La mayoría de usuarios del correo electrónico emplean esta forma de comunicación (también) para asuntos privados. Esto no crea problemas, ya que en los mensajes privados no importa, por ejemplo, la apariencia de la dirección. Da igual si delata su lugar de residencia o quién es su proveedor de Internet (por ejemplo, *juanito@yahoo.es*). Lo importante en la dirección de e-mail privada es que siga vigente durante todo el tiempo posible, de modo que sirva a sus conocidos para ponerse en contacto con usted incluso tras un lapso prolongado de silencio. Tenga cuidado de utilizar esta dirección exclusivamente para los mensajes privados y no la comunique nunca en la Red como dirección de contacto (por ejemplo para concursos). Así evitará que acabe en las listas de la publicidad on-line y se protegerá de los mensajes publicitarios.

En las direcciones de correo electrónico que se empleen para negocios importa mucho la apariencia externa. Por ejemplo, si usted en calidad de fundador busca socios capitalistas para su proyecto de negocio, una dirección de correo electrónico de la universidad donde acabara recientemente la carrera no causaría precisamente buena impresión. Naturalmente, lo más profesional sería disponer de un dominio propio con el nombre que vaya a llevar la empresa y tener la correspondiente dirección de correo electrónico, pero también puede bastar una dirección neutra de un proveedor de correo electrónico gratuito. Por razones de organización resulta recomendable separar los mensajes privados de los de trabajo. De este modo, los e-mails entrantes pasarían automáticamente a distintos buzones de correo, uno de los cuales podría consultar desde la oficina y el otro desde casa. Además, la dirección de e-mail del trabajo sólo debería ser comunicada a aquellos con los que hagamos negocios, para evitar ser importunados con e-mails en el ordenador de Internet de la empresa, o incluso recibir ataques sobre el mismo.

Direcciones de correo electrónico publicadas en la Red

La publicación de una dirección de correo electrónico en la Red (por ejemplo en su página web personal), supone un considerable inconveniente. Al contrario de lo que ocurre con una dirección privada, protegida cuidadosamente, usted no controla de ninguna manera quién consulta la dirección de la Red. Algunas agencias de publicidad emplean, por ejemplo, buscadores especiales, que rastrean las páginas web en busca de direcciones de correo electrónico (el símbolo característico de @ les facilita mucho el trabajo). Si usted quiere evitar la recepción de mensajes publicitarios por e-mail no debería publicar sus direcciones privadas y

comerciales en páginas web. Utilice en su lugar direcciones adicionales que pueda cambiar siempre que lo necesite. Si surge por este camino un contacto privado o comercial serio, siempre le podrá comunicar la dirección alternativa. Además, las direcciones divulgadas públicamente deberían ser lo más neutras posible y no revelar detalles sobre su persona, como podrían ser el lugar de residencia o la empresa donde trabaja.

Direcciones de correo electrónico en el chat

La mayoría de los chat exigen para darse de alta una dirección de correo electrónico. Estas direcciones también están al alcance de otros chateadores, de modo que estos podrán establecer contacto privado con usted. La idea en sí está bien pero, por desgracia, usted no puede controlar quién va a dirigirse a usted. Si es esa chica tan maja (o ese chico tan simpático) con la que estuvo flirteando anoche durante dos horas, ¡de maravilla! Pero, ¿y si es el tipo mordaz con quien tuvo ayer una pelea on-line, que ahora quiere seguir la disputa por otros cauces? También en estos casos es recomendable emplear una dirección especial para chatear, que no revele nada sobre usted y que pueda cancelar y cambiar en cualquier momento, si empieza a darle la lata algún chiflado. Y a la chica encantadora, siempre le podrá revelar la dirección alternativa.

Direcciones de correo electrónico para compras y concursos on-line

Si usted quiere ponerse voluntariamente a merced de la industria publicitaria, lo mejor sería participar en todos los concursos on-line que pueda encontrar. Y es que a muchos de estos concursos sólo les interesan las direcciones de los participantes. Después, pueden ser vendidas por pingües beneficios a las agencias que financian los premios ofrecidos y algunas cosas más. Para estos asuntos recomendamos emplear preferentemente direcciones especiales, que puedan ser canceladas si se hace insufrible la proporción entre mensajes publicitarios e e-mails "desgraciadamente perdidos". En ese caso lo mejor es conseguir otra dirección gratuita y empezar de nuevo.

También para las compras on-line se exige muchas veces una dirección, que se emplea para confirmar pedidos, notificar el estado de los mismos y similares. Las tiendas virtuales serias no deberían abusar de las direcciones para enviar correos electrónicos publicitarios. Pero, desgraciadamente, no todas son tan serias. Además, las tiendas virtuales tienen un truco muy apreciado: en alguna parte del formulario donde hay que indicar la dirección de correo electrónico se oculta una opción poco llamativa. Sirve para indicar si también se quiere "recibir información sobre los productos del proveedor y sus socios" por correo electrónico. Hablando claro: publicidad. Esta opción casi siempre está redactada con

tal enrevesamiento, que hay que leerla varias veces para saber si conviene marcarla o no.

TRUCO

Administrar hábilmente varias direcciones de correo electrónico

La mayoría de proveedores de direcciones gratuitas de e-mail facilitan un servicio de direccionamiento. Consiste en que usted da una dirección a la que deban ser remitidos automática e inmediatamente todos los mensajes recibidos. Si en cada dirección adicional indica el mismo destino para el direccionamiento, todos los mensajes acabarán en un mismo buzón de correo, donde los podrá descargar del modo habitual.

Además, algunos proveedores de direcciones gratuitas disponen de un servicio de recogida POP. Éste puede recoger automáticamente de los diferentes buzones todos los mensajes recibidos y ponerlos a disposición en un único buzón de correo. Aunque esto sólo funciona, si los distintos buzones de correo pueden ser llamados a través de un servidor POP3, no en los servicios de e-mail basados exclusivamente en la Red.

8. Navegar con más seguridad – anónimo y seguro en Internet

8.1 La víctima de cristal – investigación personal en internet 454
El instrumento estándar: el buscador 454
Averiguar direcciones de correo electrónico 458
Buscar en los archivos de noticias 460
Averiguar la ubicación utilizando la guía telefónica 463

8.2 Galletas amargas – las cookies, un riesgo para la seguridad 465
Funciones y peligros 466
Verificar y borrar las cookies existentes 468
Las funciones cookie de los navegadores 469
Una cómoda protección con Cookie Pal 475

8.3 Anónimo por la Red – navegar sin dejar huellas 481
¿Qué información está en juego? 481
Haga la prueba: ¡Esto es lo que revela su navegador sobre usted! 482
Así se hace: navegar de incógnito por la Red 486
Para los que quieran estar muy seguros: el software Anonymizer 490

Internet funciona en ambas direcciones. No sólo puede consultar datos, sino que también otros pueden informarse sobre usted. La creciente comercialización de Internet hace que esté plagado de estrategias de marketing, que ven en cada internauta un cliente en potencia. Como siempre, los expertos en marketing quieren saber todo lo que puedan sobre sus clientes, para poder inundarles de un modo selectivo con publicidad y ofertas, por lo que no dejan pasar ninguna oportunidad para recopilar información sobre los intereses y hábitos de los internautas. Desgraciadamente, muchas veces esto invade el entorno privado. También para los curiosos que le acechen y quieran saber más sobre usted, Internet es una primera dirección. Si usted participa activamente en grupos de noticias o foros similares, o incluso posee su propia página web, es muy sencillo elaborar un perfil suyo que tal vez sirva a los hackers como punto de partida para el social hacking. En este capítulo queremos mostrarle en qué puntos acechan los detectives y estrategas de mercado, y cómo puede proteger sus datos personales y confidenciales.

8.1 La víctima de cristal – investigación personal en Internet

Internet es una gigantesca fuente de información, que también puede revelar datos sobre personas concretas. En función de lo activo que sea un usuario en Internet deja sus huellas en páginas web o grupos de noticias. Algunas de estas fuentes poseen una memoria extraordinariamente duradera. Las páginas web existen hasta que su autor las actualice o borre. Las páginas generadas de modo automático, como por ejemplo archivos de chat o libros de visitantes, pueden conservarse perfectamente durante años. La mayoría de los grupos de noticias son recopilados en archivos, que guardan cada contribución individual. Todas estas fuentes de información pueden servir a los hackers como punto de partida para un ataque personal. Una vez averiguado el nombre, el alias o una dirección de correo electrónico de la víctima, se puede iniciar con estos datos una búsqueda en Internet para recopilar toda la información posible. Muchas veces esto ya basta para lanzar un ataque y, de no ser así, al menos sirve de base para seguir adelante con el social hacking (vea el Capítulo 1). Y no sólo para los hackers supone Internet una fuente de información útil: sobre todo en el entorno de IT, se rumorea que más de un jefe de personal ya se ha informado así sobre la pasada actividad en Internet de los aspirantes a un puesto.

En las siguientes páginas queremos mostrarle algunas posibilidades para indagar en Internet sobre personas concretas. No quisiéramos que esto fuera entendido como un manual sobre cómo sacar a la luz los secretos inconfesables de compañeros de trabajo, vecinos o el nuevo novio de la hija. Lo que nos interesa es, que usted vea las posibilidades disponibles para obtener información. Queremos que esto le sirva de ayuda para no dejar huellas que puedan convertirle a usted mismo en víctima de un ataque personal. Quizá podría probar con su propio nombre los métodos descritos. Así verá todo lo que podría averiguar sobre usted un fisgón.

El instrumento estándar: el buscador

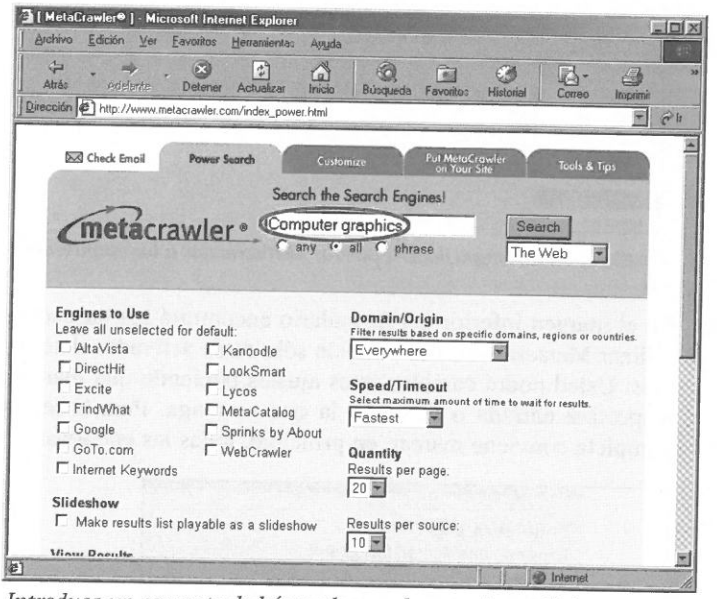
Un buscador es, en principio, el mejor recurso, si se conoce un nombre, un alias o una dirección de correo electrónico como punto de partida. Con los buscadores se pueden encontrar todas las páginas web en las que aparezca ese nombre o esa dirección. Las páginas halladas pueden ser visitadas directamente para comprobar si todos esos datos corresponden realmente a la persona buscada. No es aconsejable limitarse a un solo buscador, sino usar el mayor número posible. Antes de ejecutar sucesivamente el procedimiento de localización en varios buscadores, con lo que después habría que bregar con los aciertos múltiples, lo mejor sería emplear desde el principio un metabuscador. Este es un servicio de búsqueda especial que no dispone de bases de datos propias, sino recurre a la

información de otros buscadores. Remite la consulta introducida a gran número de buscadores y espera su respuesta. Una vez recibida, resume los resultados y los presenta con claridad.

Buscar personas con el metabuscador Metacrawler

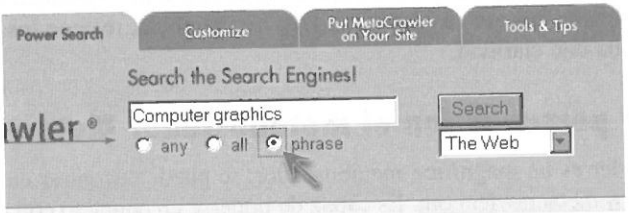
Metacrawler es un magnífico metabuscador, se puede encontrar en la dirección http://www.metacrawler.com. Es capaz de ponerse en contacto con unos 13 buscadores y transmitirles a éstos la consulta correspondiente. Usted podrá saber por la página inicial de cada servicio qué buscadores son.

1. Para buscar con Metacrawler llame en el navegador web la página inicial de este servicio bajo la dirección http://www.metacrawler.com. A continuación, sitúese en la pestaña *Power Search*.
2. En el campo de búsqueda introduzca el concepto de búsqueda deseado.



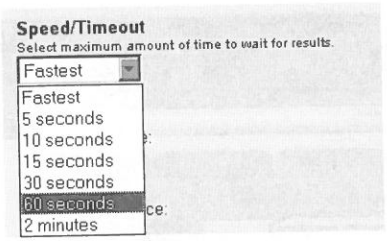
Introduca un concepto de búsqueda por el que quiera solicitar una búsqueda paralela.

3. Si usted busca un nombre compuesto por varias partes (es decir, nombre y apellidos), debería emplear un operador de búsqueda. Éste se encargará de encontrar sólo aquellas páginas web donde figuren juntos los dos nombres. Para ello, en el apartado inferior del concepto de búsqueda, elija la opción *phrase*. Por supuesto, si usted emplea un único concepto de búsqueda todo esto no le afectará.



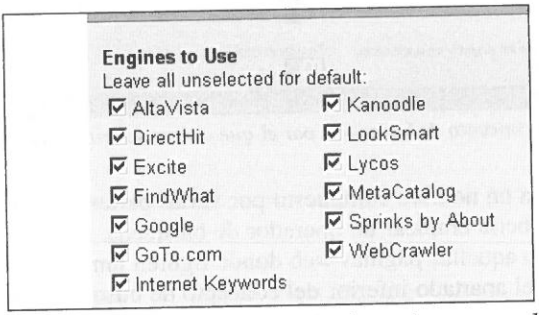
Elija el tipo de vinculación cuando haya varios conceptos de búsqueda.

4. Es importante que ajuste X segundos como tiempo máximo de búsqueda inicial. Este valor decide el límite de segundos que deberá esperar Metacrawler hasta que lleguen las respuestas de los otros buscadores. Si elige aquí un valor demasiado bajo, usted mismo se privará de los mejores resultados.



Decida cuánto tiempo deberá esperar Metacrawler a las respuestas de los buscadores.

5. En el margen inferior del formulario encontrará los buscadores que puede utilizar Metacrawler. Por omisión sólo están activados determinados servicios. Usted podrá cambiar estos ajustes poniendo una marca delante de la respectiva entrada o quitando la que ya tenga. Para hacer una búsqueda completa conviene marcar, en principio, todas las entradas.

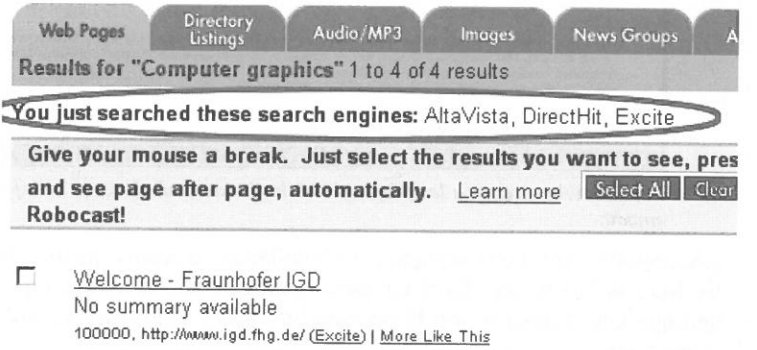


En el índice de buscadores puede ajustar los recursos de búsqueda que deban ser consultados.

6. Ahora, si todo está especificado y ajustado como usted quería, vuelva al comienzo del formulario de búsqueda y haga clic sobre el botón *Search*.

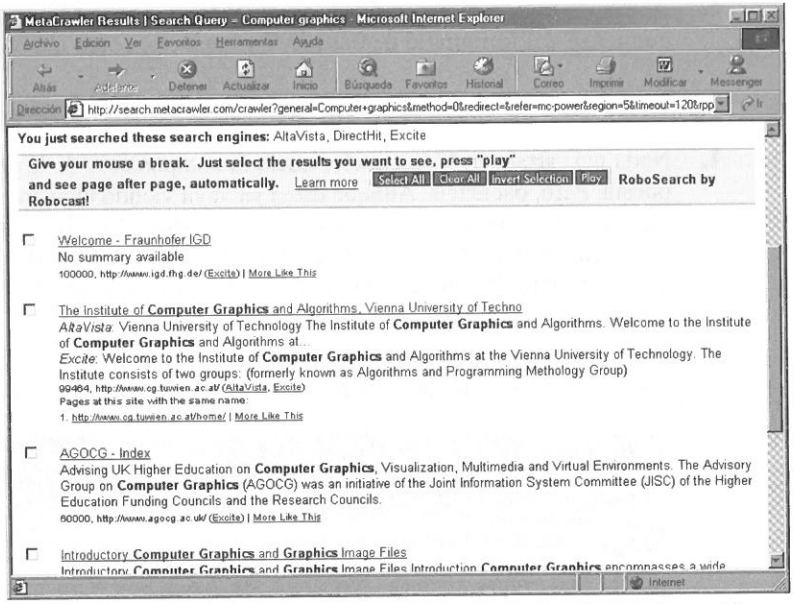
Evaluar los resultados de búsqueda de Metacrawler

1. Nada más arrancar, Metacrawler inicia la composición de la página de respuesta. Pero, paciencia. Aunque usted ya vaya viendo algo en el navegador, esto no quiere decir que los resultados ya estén ahí. Metacrawler sólo le entretiene durante el tiempo de espera con algunas informaciones y sugerencias útiles. Cuando al fin lleguen los resultados la página iniciada simplemente será alargada.
2. En primer lugar Metacrawler le presentará una breve estadística de la búsqueda, indicando qué buscadores intervinieron en las páginas encontradas.



En primer lugar, Metacrawler le da un pequeño resumen estadístico de los resultados obtenidos.

3. Cuando Metacrawler termina, amplía la página de respuesta con los datos correspondientes, que ahora son el título y la dirección de las páginas web halladas. Para cada entrada recibirá la información más importante como URL, título de la página, un breve resumen, fecha, tamaño y servicio de búsqueda que comunicó ese acierto. Si no aparecen todos estos datos en todas las entradas es porque Metacrawler sólo puede transmitir la información que él mismo ha obtenido de sus colaboradores.
4. Si una página ha sido hallada por varios servicios, también recibe varias entradas para esa página. Esto le permitirá establecer una excelente comparación entre los diferentes buscadores y sus resultados.



Metacrawler presenta las páginas web halladas y añade toda la información que pueda.

Ahora podrá entrar en las páginas web halladas haciendo clic directamente sobre los links del resultado. Es obvio que, a partir de ahora, analizar qué páginas tienen que ver realmente con la persona buscada y cuáles no, es una tarea que le corresponde a usted.

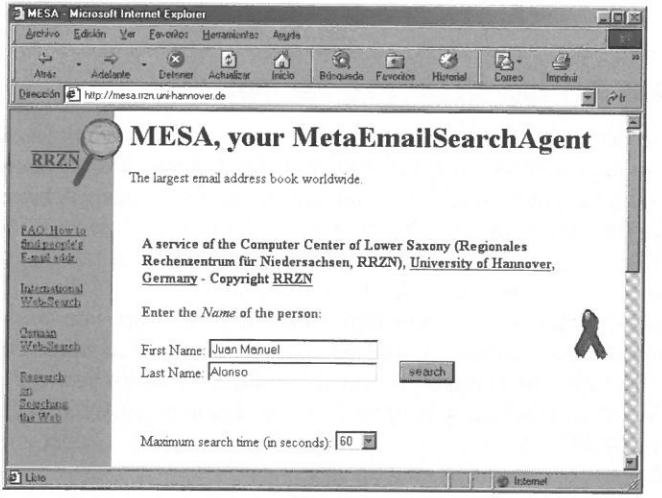
Averiguar direcciones de correo electrónico

Según ha demostrado la experiencia, las direcciones de correo electrónico están especialmente cotizadas, y no sólo por los estrategas publicitarios, también por los hackers. A fin de cuentas, una dirección de correo electrónico ofrece un excelente punto de ataque. Por una parte, brinda la posibilidad de hacer llegar un e-mail a la víctima. Esto, a su vez, permite sabotear el ordenador mediante contenidos activos o infiltrarse en él, colando tal vez un virus informático o un troyano. Aparte de esto, la dirección de correo electrónico puede dar al atacante información sobre la red a la que pertenece el atacado. Así, el hacker ya sabe en qué ordenadores debe buscar puntos débiles. Y finalmente, se puede emplear una dirección de correo electrónico para poner en circulación mensajes falsificados con el nombre de la víctima. Lo que supone prácticamente suplantar la identidad virtual de otro.

Encontrar direcciones de correo electrónico con MESA

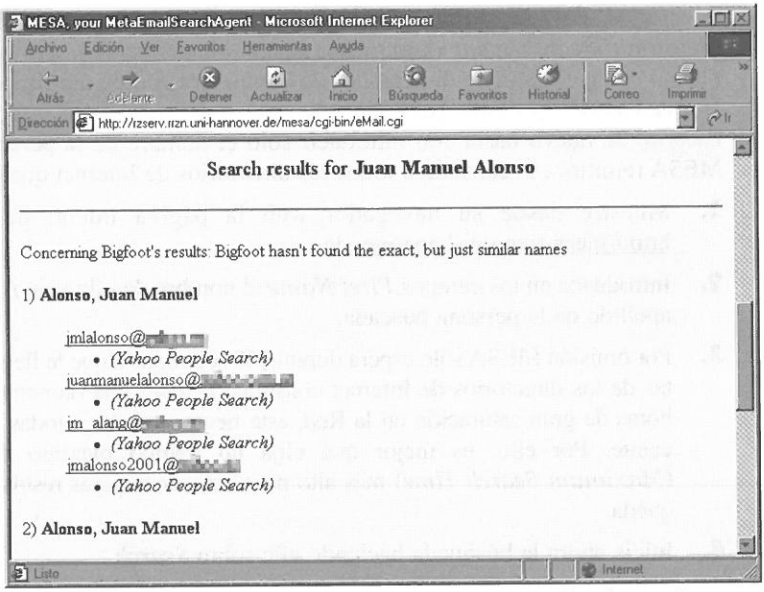
También es posible encontrar direcciones de correo electrónico a través de Internet. Igual que en la vida "real" disponemos de listines de teléfono, también en Internet hay directorios de correo electrónico donde se puede averiguar la dirección de e-mail que corresponda a un nombre. También en este caso se recomienda recurrir a un metabuscador en lugar de recorrer uno a uno todos los directorios. Para eso sirve el hermano pequeño de *Metacrawler*: *MESA*, el *MetaEmailSearchAgent* (http://mesa.rrzn.uni-hannover.de), que se define a sí mismo como el listín de direcciones de correo electrónico más importante. Con él usted puede explorar paralelamente una amplia serie de directorios. Para hacerlo, de nuevo basta con introducir sólo el nombre de la persona buscada. MESA remitirá esa consulta a todos los directorios de Internet que conozca.

1. Muestre desde su navegador web la página inicial de MESA en http://mesa.rrzn.uni-hannover.de.
2. Introduzca en los campos *First Name* el nombre de pila y en *Last Name* el apellido de la persona buscada.
3. Por omisión MESA sólo espera durante 60 segundos a que le lleguen respuestas de los directorios de Internet consultados. Pero precisamente durante las horas de gran saturación en la Red, este tiempo resulta a todas luces insuficiente. Por ello, es mejor que elija un tiempo máximo de búsqueda (*Maximum Search Time*) más alto para obtener mejores resultados de búsqueda.
4. Inicie ahora la búsqueda haciendo clic sobre *Search*.



El formulario de búsqueda de MESA, con el que usted puede explorar simultáneamente multitud de listines de direcciones.

5. Ahora MESA transmite su consulta a los directorios de correo electrónico que conozca. Después espera los resultados durante el tiempo indicado, recopila las respuestas de los directorios y, al mismo tiempo, las depura. De este modo elimina los aciertos repetidos que hayan sido hallados en varios directorios. A continuación le presenta como página web en el navegador los resultados ya clasificados.



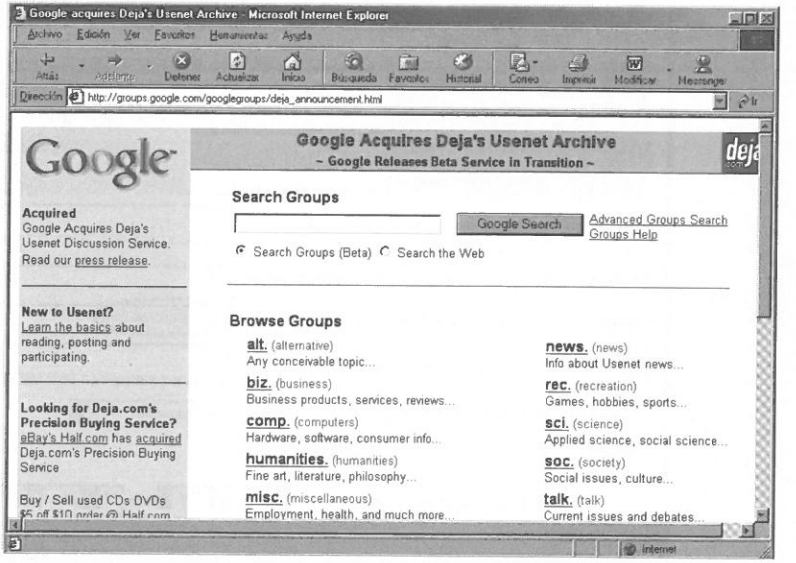
MESA depura los resultados de los diferentes listines de direcciones y los presenta.

Buscar en los archivos de noticias

Tampoco los mensajes de grupos de noticias cuyo ciclo vital haya expirado, desaparecen para siempre en el nirvana de datos. Algunas iniciativas se han afanado en recopilar el sinfín de datos, informaciones, opiniones y debates, para almacenarlo permanentemente. Ponen a disposición esta colección dentro de un archivo, que cualquiera puede utilizar. Y aquí no sólo se puede buscar por temas, sino también por autores. Así, sabiendo un nombre o una dirección de correo electrónico, se puede averiguar rápidamente en qué grupos de noticias participó una persona en el pasado, e incluso obtener las contribuciones de ese participante. Esto permite elaborar un perfil completo sobre los intereses de una persona. Si a ésta, además, se le escapó en sus artículos alguna información personal, quizá podría haber datos delatores para quien quiera hacer social hacking, por ejemplo para descifrar contraseñas.

Explorar el archivo de noticias Deja.com en busca de autores

1. El archivo de noticias quizá más extenso lo encontrará desde su navegador web bajo http://www.deja.com o http://www.google.com.

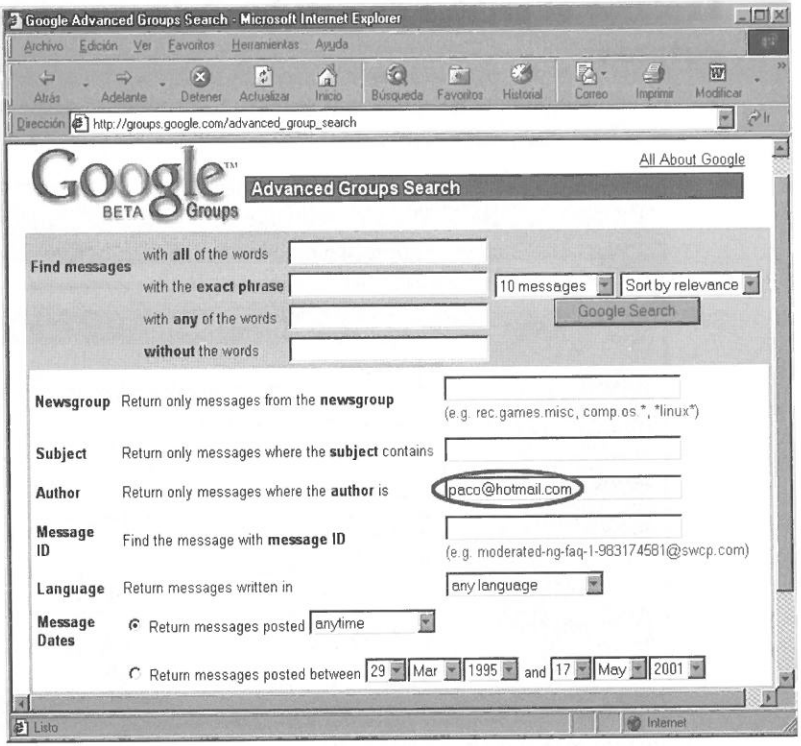


Aspecto general del buscador Google.

2. Con eso llamará al formulario de búsqueda, donde podrá introducir enseguida el concepto buscado. Aunque si lo que desea es buscar una persona concreta, le servirá más el link *Advanced Groups Search*.

Llame desde el formulario de búsqueda Advanced Groups Search para realizar una búsqueda selectiva.

3. Con esto abrirá una nueva página, que permite ajustar los parámetros de búsqueda con mucha más exactitud y flexibilidad.



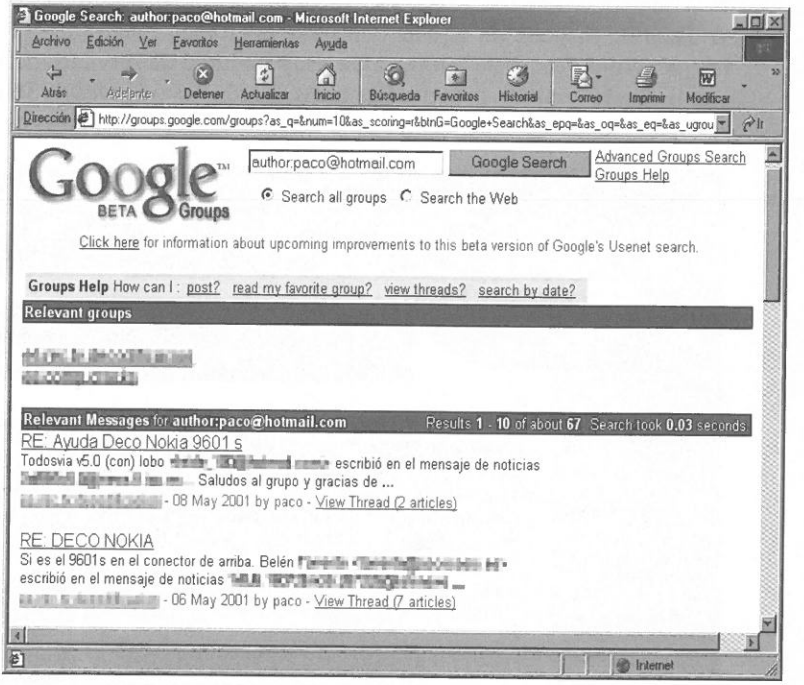
Power Search permite una búsqueda muy selectiva.

4. Aquí resulta especialmente interesante el campo *Author*, donde se puede introducir la dirección de correo electrónico de la persona cuyas contribuciones nos interesen. De no conocerse la dirección sino el nombre habría que emplear a este como concepto de búsqueda. Esto también arroja una alta probabilidad de dar con contribuciones de esa persona. Igualmente se pueden encontrar contribuciones de respuesta a una noticia de la persona buscada, con lo que finalmente se acabaría dando con la pista correcta.

5. El resto de opciones y parámetros de búsqueda pueden servir para acotar más la indagación. Por ejemplo, se puede indicar en qué idioma irían redactadas las contribuciones buscadas y de qué grupo de noticias o período deberán proceder.

6. Ponga en marcha ahora la búsqueda haciendo clic sobre *Google Search*.

7. En los resultados de búsqueda deja.com le presentará los aciertos ordenados por la fecha de publicación, figurando en primer lugar las contribuciones más recientes.



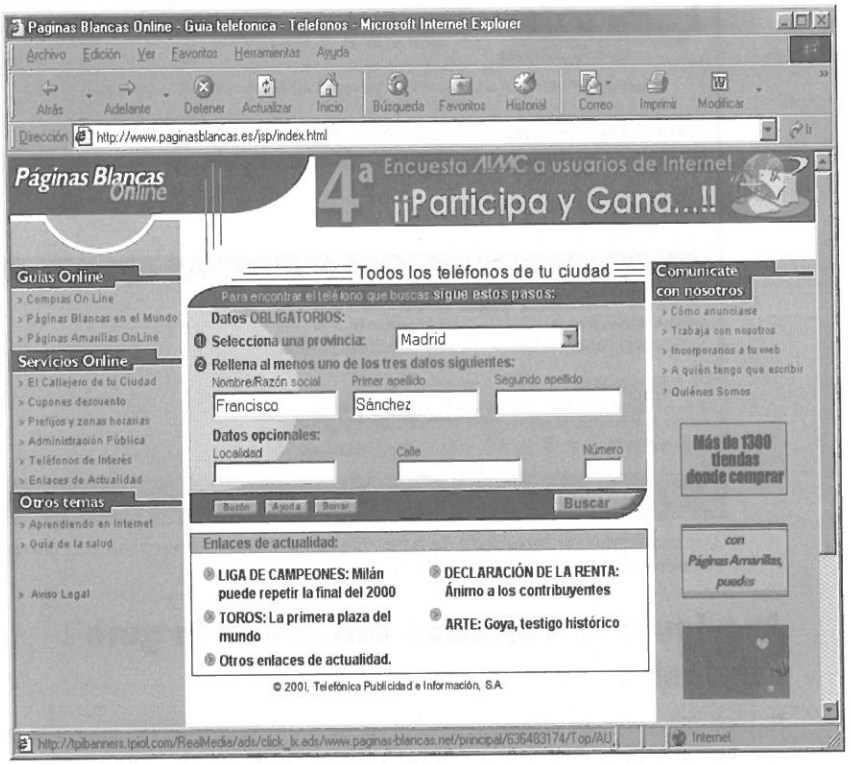
Los resultados de búsqueda de http://www.google.com presentan con claridad las contribuciones de noticias halladas.

Averiguar la ubicación utilizando la guía telefónica

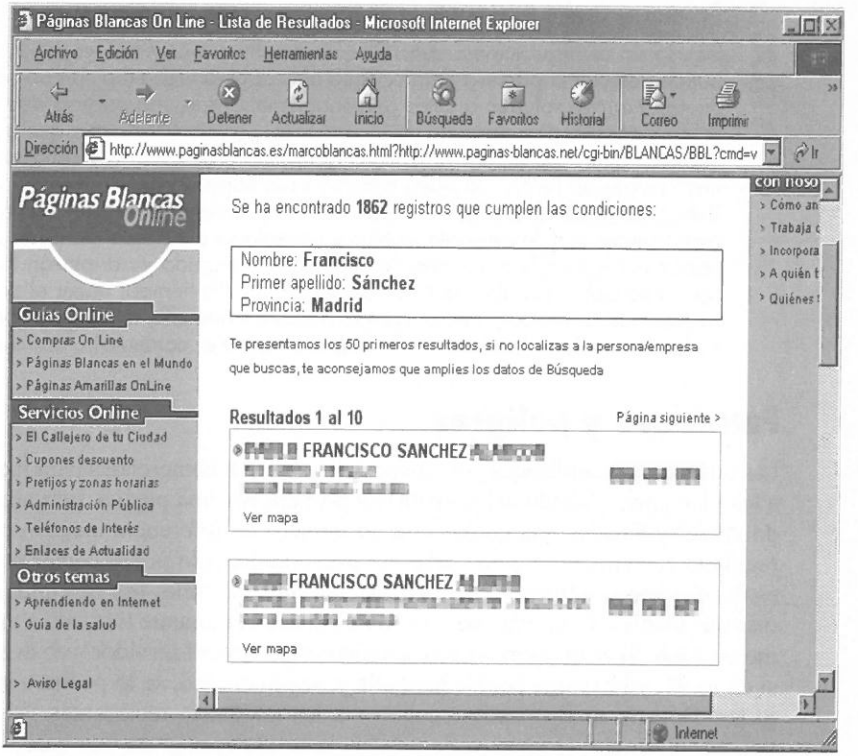
Si para perpetrar un ataque personal se necesita saber dónde vive una persona, casi siempre sirve de ayuda un vistazo a la guía telefónica. Aunque no exista ningún listín que abarque el país entero, hoy en día los CD de la guía telefónica ya permiten una cómoda búsqueda por todo el territorio nacional. Disponiendo de un nombre y siempre que la persona en cuestión figure en la guía de teléfonos, se la encontrará con toda seguridad. Y cuando se conoce el teléfono enseguida se obtiene mucha más información. A fin de cuentas, ahora se puede localizar a la persona. Mucha gente también quiere que incluyan su dirección en la guía. Con eso ya no queda ninguna pregunta por contestar. Pero incluso sin estos datos se puede avanzar. En cualquier caso, el prefijo ya revela el lugar de residencia o, si se trata de una ciudad grande, incluso el barrio. A veces, el propio número per-

mite deducir el distrito o hasta la calle, aunque para eso hacen falta ciertos conocimientos técnicos. Además, hoy en día la red totalmente digitalizada permite trasladarse con el número de teléfono dentro de una zona de código territorial, de modo que el prefijo no siempre es significativo.

Si usted no dispone de un CD con listín telefónico podrá recurrir de nuevo a Internet como fuente de información. Hay multitud de servicios de información online donde se puede indagar. Las guías telefónicas oficiales de Telefónica, por ejemplo, pueden ser consultadas bajo http://www.paginasblancas.es.



En la dirección http://www.paginasblancas.es.



... se pueden averiguar números de teléfono.

8.2 Galletas amargas – las cookies, un riesgo para la seguridad

Un tema muy controvertido en Internet son las cookies. Muchas páginas web las utilizan y casi nadie sabe muy bien para qué sirven, incluso nos vemos obligados a aceptarlos y pueden ser nocivos. Si permitimos el empleo de cookies sin restricciones existe el peligro de que nuestro comportamiento sea espiado en la Red. Si por el contrario lo impedimos, por ejemplo, en muchas tiendas virtuales, nos quedaríamos fuera. También el término medio, es decir, decidir individualmente para cada cookie, acabaría sacándonos pronto de quicio porque, a la hora de navegar por la Red, seríamos molestados constantemente con advertencias y consultas del navegador. Pero todo esto no tiene porqué ocurrir. En este apartado vamos a adentrarnos en los secretos de las cookies, mostrándole cómo protegerse de ellas con eficacia y sin sacrificar la comodidad.

TRUCO

Detectar el empleo de cookies

Incluso sin configuraciones concretas ni un software especial, casi siempre se puede detectar a primera vista cuándo una página web emplea cookies. Siempre que le saluden a usted personalmente desde una página web o aparezca cualquier otra variante de información personalizada, sin que usted se hubiera registrado en esa página con su nombre de usuario y contraseña, hay cookies en juego. Un buen ejemplo es la librería online Amazon (http://www.amazon.com). Si usted había hecho alguna vez un encargo como cliente y, más adelante, vuelve a conectarse allí desde el mismo ordenador, enseguida le saludarán de modo personalizado y adaptarán las ofertas especiales a sus aficiones personales. Al mismo tiempo, hacer el pedido resultará más rápido y menos complicado. Actualmente, muchas tiendas virtuales ya emplean técnicas similares para mantener contentos a sus clientes.

Funciones y peligros

Las cookies son empleadas por muchas páginas web comerciales para reconocer a los visitantes. Cuando usted visita por primera vez una página, será almacenado en su ordenador una cookie con un número de referencia inequívoco. Está regulado con exactitud cómo debe ser esta cookie: sólo podrá contener texto – es decir, letras y números - no información binaria como, por ejemplo, programas ejecutables. El tamaño de las cookies queda claramente limitado a un máximo de 4 Kb. Si en el futuro vuelve a visitar esa oferta, el servidor web averiguará si en su PC ya hay una cookie para ella y, según el caso, se lo pedirá a su navegador. De este modo puede reconocer a los visitantes recurrentes. Al mismo tiempo, junto con el número de referencia se almacenan en una base de datos informaciones concretas, como por ejemplo el tipo de ofertas o novedades por las que usted muestre especial interés. Esto permite adaptar dinámicamente la página web a sus necesidades, o insertar banners publicitarios en función de las preferencias de usted. Muchas veces las tiendas virtuales también trabajan con cookies para garantizar que a cada visitante le sea asignada su cesta de la compra intransferible.

INFO

¿Son peligrosas las cookies?

Las cookies no representan ningún peligro para su PC, en el sentido de los virus o troyanos. A fin de cuentas no incluyen instrucciones binarias ni pueden causar otro tipo de daños. Aunque sí pueden ser aprovechadas por los hackers, junto con otras técnicas, para espiar a su ordenador. Para ello, un programa de espionaje archivaría información en una cookie, que podría ser transmitida al servidor web del hacker. Aunque es mucho mayor el peligro para el entorno privado. Y es que a un experto las cookies le revelan con suma exactitud las páginas web que usted visitó. Ni siquiera necesitaría tener acceso a su PC, ya que las cookies pueden ser llamadas desde cualquier servidor que conozca la denominación correcta. De este modo el operador de

una tienda virtual puede detectar, por ejemplo, si usted también compra a la competencia y hasta podría usar fraudulentamente esa información. ¿Quizá usted visite de vez en cuando páginas web, de las que otros no deban saber nada? Las cookies almacenadas podrían delatarle. Por eso, a la hora de manejar estas migajas de información se recomienda cierta prudencia.

Así se programan las cookies

Las cookies son parte integrante del lenguaje script *JavaScript*. Éste facilita funciones para generar y llamar cookies. El objeto JavaScript decisivo para eso se llama *document.cookie*. El modo de proceder básico es el siguiente:

1. Nada más abrir la página de inicio se pregunta con *document.cookie* si en el ordenador del visitante existe una cookie para esa página. En caso afirmativo, el objeto *document.cookie* recibe el valor que esté almacenado en la cookie del ordenador del visitante. De lo contrario quedará vacío.
2. Si tras la consulta el objeto contiene un valor, éste puede ser analizado con los métodos habituales de JavaScript y tal vez se pueda averiguar un número de visitante. Éste podría ser cotejado con una base de datos, en la que se almacenen datos más extensos sobre ese visitante.
3. Si el objeto no contiene ningún valor, significa que el visitante accede a esa página por primera vez y aún no hay datos suyos. En este caso, de nuevo se puede emplear el objeto *documento.cookie* para depositar una cookie. Para hacerlo, simplemente se asigna al objeto el valor correspondiente, como por ejemplo:

   document.cookie = "nº de visitante=123456; expires= Wed, 11 Mar 2002 18:17:28 GMT;"

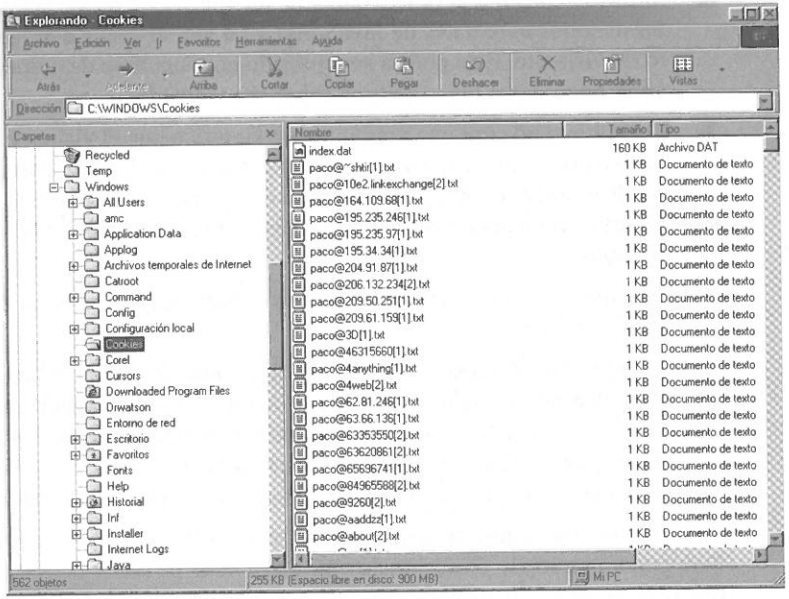
   La información en sí se indica con el nombre del valor (*nº de visitante*) y el contenido del valor *(123456)*. Además, hay que especificar en *expires* una fecha de caducidad para la cookie. Por regla general, los navegadores no aceptan cookies que no lleven esta fecha. Con esto, en la siguiente visita se puede analizar la cookie existente y reconocer al visitante.

Sólo con las funciones de JavaScript la técnica de cookies tiene poco sentido. Para poder emplearla profesionalmente siempre debe haber detrás la conexión a una base de datos que permita analizar o seguir procesando la información obtenida de las cookies. Por lo que esta técnica sólo suele ser empleada por sitios web importantes y profesionales.

Verificar y borrar las cookies existentes

Las cookies son pequeños bloques de información que los servidores web ordenan almacenar al navegador web en su PC como archivos. Visto con un enfoque técnico, el servidor web transmite la información de las cookies al navegador web y le solicita guardar esa información bajo un nombre concreto. Tanto Internet Explorer como Netscape Navigator cumplen esta petición de forma estándar. Navigator emplea para ese fin un archivo de texto llamado *Cookies.txt*, que genera por separado para cada usuario de Windows. Internet Explorer guarda las cookies en una carpeta especial para *Cookies*, integrada en el directorio principal de Windows. Quizá le convendría echar un vistazo y comprobar cuántas cookies ha acumulado ya en su ordenador.

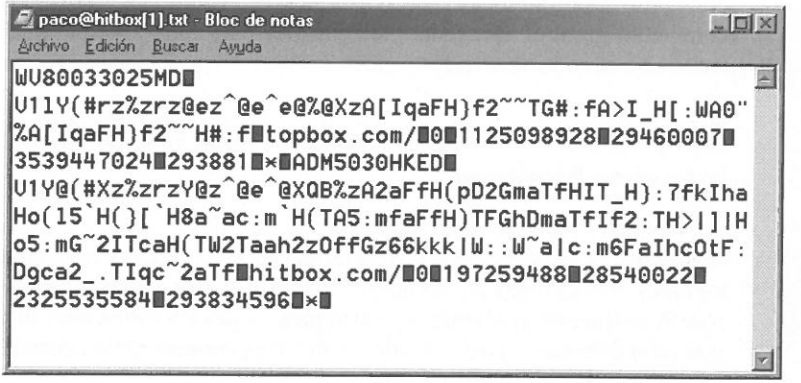
1. Arranque el Explorador de Windows y abra la carpeta de Windows (casi siempre *c:\windows*). Allí encontrará la carpeta *Cookies*, cuyo contenido podrá visualizar.



Internet Explorer almacena las cookies como pequeños archivos de texto.

2. La carpeta contiene un archivo llamado *index.dat*, que proporciona una relación de todas las cookies almacenados. Pero las verdaderas cookies y su información están guardadas en esa carpeta como multitud de archivos diminutos. La mayoría de éstos ocupan menos de 1 Kb, de modo que en condiciones normales no hay que preocuparse por el espacio en memoria.

3. Las cookies almacenadas son archivos de texto sencillos, que puede abrir con cualquier editor de textos. Aunque al hacerlo, comprobará que en la mayoría de los casos el contenido sólo consiste en números y letras aparentemente sin sentido. Aunque muchas veces la dirección del sitio web responsable viene en texto claro.



Este es el aspecto que tiene el contenido de un archivo cookie.

Muy importante: ¡bajo ningún concepto caiga en la tentación de iniciar una acción de limpieza recurriendo a la función de borrado! Los contenidos de la carpeta y los del archivo *index.dat* deben concordar siempre. Si usted se limita a borrar los archivos de cookies, Internet Explorer podrá desestabilizarse y reaccionar con caídas. Para borrar las cookies hay un software especial del que hablaremos más adelante.

Las funciones cookie de los navegadores

Contra el uso de cookies por las páginas web no se puede hacer nada. De modo que la cuestión se reduce a cómo debe usted reaccionar ante estas migajas de información. Básicamente, dispone de tres estrategias:

- Si usted no teme a las cookies, podrá autorizar su empleo globalmente. En ese caso, el correspondiente tráfico de datos tendrá lugar en segundo plano, sin que usted advierta nada. Aunque con esto también perderá el control sobre quién almacena o consulta determinada información.
- Si usted es un enemigo declarado de las galletas electrónicas puede impedir su empleo, también globalmente. Entonces su navegador web ignorará todas las consultas relacionadas con cookies. Esto supone una protección óptima contra abusos, aunque ya no podrá acceder a determinadas páginas web. No obstante, en la mayoría de los casos se pueden encontrar alternativas que funcionan sin cookies.

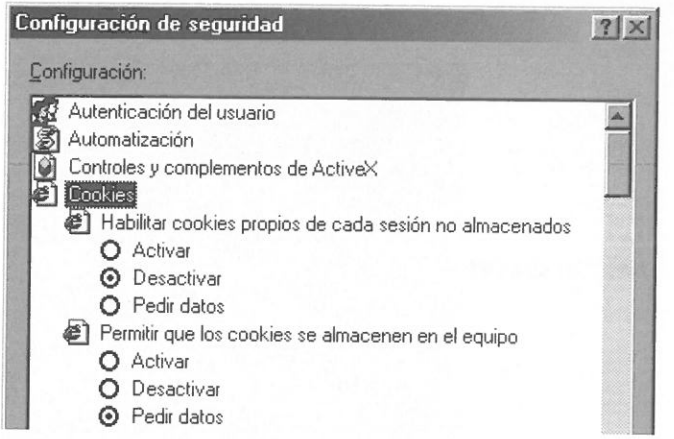
- Como siempre, el camino del medio es el mejor: deje que su navegador le advierta cuando alguien quiera escribir o leer cookies y decida para cada caso concreto. Con los navegadores web habituales esto suele ser algo engorroso, pero hay software adicional que le puede servir de ayuda.

Las versiones usuales de los navegadores web Internet Explorer y Netscape Navigator soportan todas estas posibilidades. A continuación vamos a enseñarle cómo configurar el navegador para que preste un apoyo óptimo a su política personal en cuestión de cookies.

Adaptar las configuraciones para las cookies en Internet Explorer

En Internet Explorer la configuración para cookies es parte del concepto de seguridad, es decir, para cada zona de seguridad usted puede establecer configuraciones individuales de cookies. Resulta recomendable autorizar las cookies para los sitios de confianza y restringirlas o desactivarlas para otras zonas. En este caso debería asignar los sitios web cuyas cookies quiera permitir (por ejemplo, las tiendas virtuales) a los sitios de confianza.

1. Para emprender las configuraciones de cookies en Internet Explorer abra desde *Herramientas/Opciones de Internet...* la pestaña *Seguridad*.
2. Seleccione aquí la zona de seguridad para la que desee ajustar las opciones de cookies.
3. Los niveles de seguridad predefinidos no se diferencian nada en cuestión de cookies. Da la impresión de que Microsoft no se toma demasiado en serio este peligro. Por eso, lo mejor será que conserve la configuración estándar. Después, haga clic sobre el botón *Personalizar nivel*.
4. Busque en la lista de configuraciones la entrada correspondiente a las cookies, donde encontrará dos subcategorías. *Permitir que las cookies se almacenen en el equipo* se refiere a *las cookies* permanentes que quedan para siempre en su ordenador. Las configuraciones *Habilitar cookies propios de cada sesión no almacenados* se aplica a *las cookies* temporales, que son borradas de todos modos al cerrar Internet Explorer.



Aquí decide usted la estrategia de Internet Explorer con respecto a las cookies.

5. Para las dos categorías puede *Activar o Desactivar* las cookies, o condicionar su autorización en cada caso a una *Petición de datos.*

6. Confirme los nuevos ajustes con *Aceptar.*

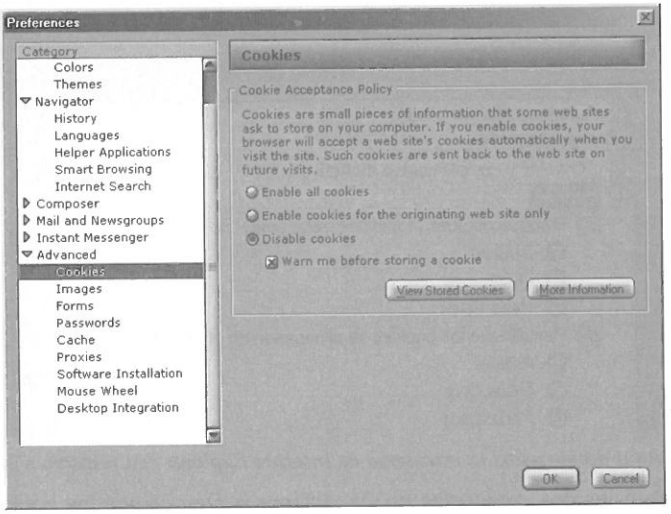
Si se ha decidido por la petición de datos, Internet Explorer le presentará en cada consulta por cookie una ventana de advertencia. Así podrá decidir si esa cookie debe ser permitida o no. Pero a la larga esto puede resultar bastante engorroso porque, de hecho, esta advertencia aparece en cada cookie y ralentiza la navegación aunque, al menos, de esta forma se puede ver la cantidad de cookies que ya circulan por la Red.

Configurar las opciones para las cookies en Netscape Navigator

En Netscape Navigator la configuración de cookies puede ajustarse de modo similar a Internet Explorer, aunque este navegador no dispone del concepto por zonas de seguridad, de modo que las opciones sólo pueden establecerse de modo global para todas las direcciones web.

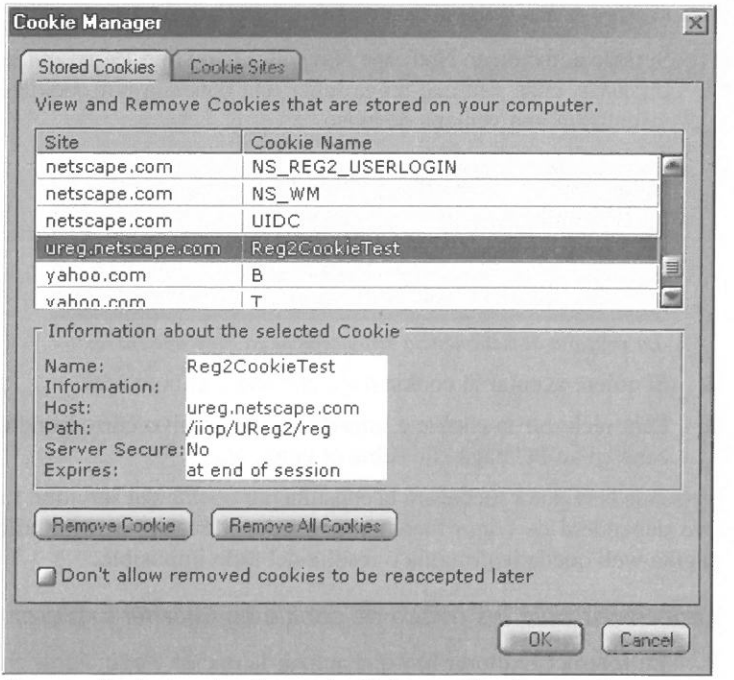
1. Para emprender la configuración de cookies en Netscape Navigator abra primero sus opciones *Edit/Preferences.*

2. Desde *Advanced* acceda al apartado *Cookies*, donde encontrará las diferentes posibilidades de configuración.



También Netscape Navigator permite dar diferentes tratamientos a las cookies.

3. *Enable all cookies.* Con esta configuración usted permite a las cookies circular libremente.
4. *Enable cookies for the originating web site only.* Esta opción es una solución que permite cookies, pero en caso de consulta sólo las devuelve al servidor del que procedan. Con ella se pretende evitar que las cookies existentes sean espiadas desde otros servidores.
5. *Disable cookies.* Si no se fía del todo de las cookies, esta opción es la mejor. Hace que Netscape Navigator rechace todas las consultas por cookie.
6. *Warn me before storing a cookie.* Esta opción adicional activa el modo interactivo para cookies, que hará que se le pida a usted autorización antes de aceptar cada cookie.
7. Haciendo clic sobre *View stored cookies* puede comprobar la cantidad de cookies almacenadas hasta ahora por Netscape Navigator y cuáles son.
8. Ahora, recibirá en una ventana adicional una lista de las cookies existentes. Si usted selecciona una de esas entradas en el área de información de la cookie elegida, aparecerán datos detallados sobre el nombre, la procedencia, el emisor y el plazo de vigencia.



Netscape Navigator visualiza en detalle las cookies almacenadas.

9. Si quiere deshacerse de una de estas galletas informáticas basta con seleccionar y hacer clic sobre *Remove cookie*. Netscape Navigator borrará los datos correspondientes de un modo fiable.

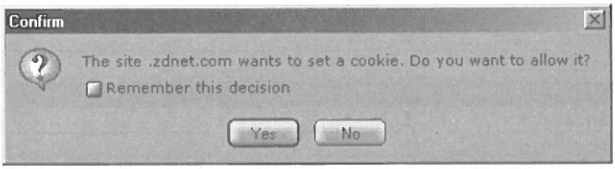
10. A continuación debería cerrar la ventana con *OK*.

Permitir las cookies sólo previa consulta

Si, aparte de consumir pasivamente las páginas web, también queremos participar de un modo interactivo, a menudo el empleo de cookies resulta inevitable. Por ejemplo, muchas tiendas virtuales necesitan las cookies para controlar la cesta de la compra de los clientes, y sin esa cesta usted no puede comprar en este tipo de tiendas, por lo que en estos casos se recomienda un acuerdo: en lugar de permitir o rechazar las cookies de modo generalizado, puede decidir en cada caso interactivamente si debe autorizarse una cookie concreta procedente de cierto servidor web. Siempre que una página web quiera colocar una cookie en su PC, el navegador web le advertirá a usted y le preguntará cómo resolver esa consulta.

Responder a los avisos de cookie en Netscape Navigator

1. Si tiene activada en Netscape Navigator la opción *Warn me before storing a cookie*, cada vez que tenga lugar una consulta por cookie el navegador visualizará una ventana de aviso.



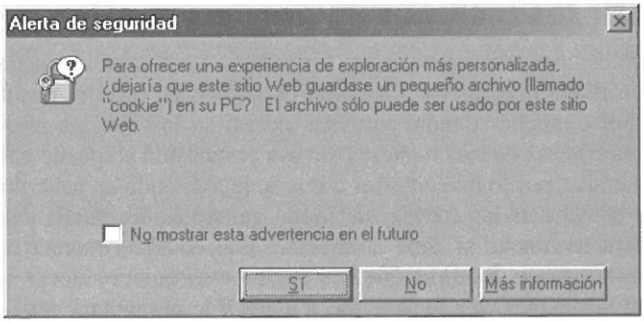
La ventana de advertencia sobre cookies en Netscape Navigator

2. Si quiere aceptar la cookie haga clic sobre el botón *OK*.
3. Para rechazar la cookie e impedir que el archivo correspondiente se almacene en su PC haga clic sobre el botón *No*.

Netscape Navigator rechazará la consulta por cookie del servidor. La reacción de éste dependerá de cómo fuera programado. Muchas veces la utilización de la página web queda restringida o resulta del todo imposible.

Reaccionar ante los avisos de cookie en Internet Explorer

1. En Internet Explorer hay que activar la opción *Pedir datos* en las configuraciones de cookies, para que cada consulta por cookie desencadene la aparición de una ventana de confirmación.
2. Si esta opción está Activa e Internet Explorer recibe la correspondiente consulta desde un servidor web, emitirá una *Advertencia de seguridad*. Desgraciadamente ésta no es tan clara como la que da Netscape Navigator y deja al usuario en la incertidumbre sobre el origen de la cookie.



También Internet Explorer puede reaccionar de modo interactivo a las consultas por cookie.

3. Si quiere permitir que la cookie sea guardado basta con hacer clic sobre Sí.
4. Si, por el contrario, no quiere aceptar la cookie, deberá decidirse por No.
5. Con *Más información* puede solicitar una explicación, que vuelve a detallar brevemente lo que significan las cookies y las opciones disponibles, pero no aborda individualmente cada cookie, sólo ofrece una información general.
6. Además, usted puede seleccionar la opción *No volver a mostrar esta advertencia en el futuro*. Puede elegirla al margen de la decisión tomada de otro modo. Hace que la primera reacción ante la consulta por cookie desde un servidor sea repetida automáticamente en todas las demás consultas, para que no sea molestado cada vez con una advertencia de seguridad. Esto resulta muy útil, ya que las cookies muchas veces no aparecen individualmente, sino en serie. Así que, en lugar de hacer clic constantemente en *Sí* o *No*, sólo hay que decidir una vez cómo deben ser tratados las cookies procedentes de ese servidor. Internet Explorer se encarga por su cuenta del resto.

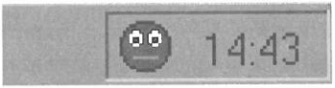
Una cómoda protección con Cookie Pal

La mejor protección contra las cookies la ofrece un software enfocado especialmente a ellos. Mantiene limpio el ordenador y, a pesar de todo, permite acceder cómodamente a las páginas web que dependan de cookies. Un producto shareware de este tipo es *Cookie Pal*, de la empresa Kookaburra Software. En http://www.kburra.com puede descargar una versión de evaluación gratuita, que trabaja con los navegadores Internet Explorer, Netscape Navigator y Opera en sus versiones actuales y, en algunos casos, también con las versiones más antiguas.

Instalar y preparar Cookie Pal

La instalación se desarrolla siguiendo los pasos habituales para los programas de Windows. Cookie Pal viene como archivo de instalación automática. Tras la advertencia sobre el acuerdo de licencia seleccione el directorio y la carpeta del Escritorio donde quiera instalar el programa. Durante la instalación Cookie Pal averigua qué navegadores hay instalados en su PC y los prepara para el trabajo conjunto. Si durante la instalación de Cookie Pal estuviera activo un navegador web, habrá que cerrarlo primero y volver a ponerlo en marcha antes de que Cookie Pal pueda funcionar correctamente. Cookie Pal trabaja sin problemas con todas las versiones actuales, y también las más antiguas, de Internet Explorer y Netscape Navigator. Por otro lado, también soporta el navegador web Opera y las versiones de navegador integradas en servicios on-line, como AOL.

Una vez concluida la instalación, llame el programa desde el menú de inicio con *Inicio/Programas/Cookie Pal/Cookie Pal*. A continuación verá en el margen inferior derecho, en la Bandeja de sistema, el icono de *Cookie Pal*, una galleta con cara. Haciendo clic sobre él con el botón derecho del mouse abrirá el menú contextual. Aquí encontrará, entre otras funciones, la opción de menú *Show*, con la que abrirá la ventana principal de Cookie Pal.

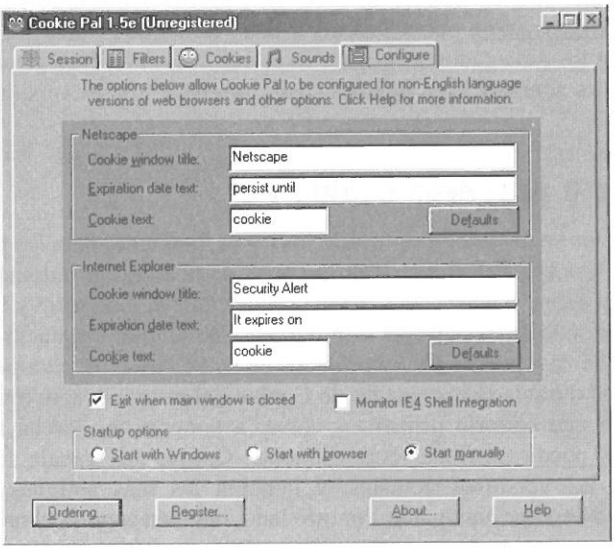


El icono de Cookie Pal en el margen inferior derecho de la Barra de tareas.

Adaptar Cookie Pal a los navegadores españoles

Como Cookie Pal es un programa en inglés, trabaja como valor por omisión con las versiones inglesas del navegador web. Si usted emplea las versiones españolas deberá adaptarlo ligeramente.

1. Abra para eso la categoría *Configure* de la ventana principal de Cookie Pal.
2. Introduzca en el campo *Netscape* o en *Internet Explorer* los valores pertinentes en cada caso.
3. Si hace clic sobre uno de los dos botones *Defaults*, hará que se inserten automáticamente los valores estándar para diversos idiomas (entre ellos también el español = *Spanish*).



Cookie Pal debe adaptarse a las versiones españolas de los navegadores web.

La siguiente tabla le revela a usted las entradas correctas para las versiones españolas actuales de los dos navegadores. Respete sin falta las letras mayúsculas/minúsculas:

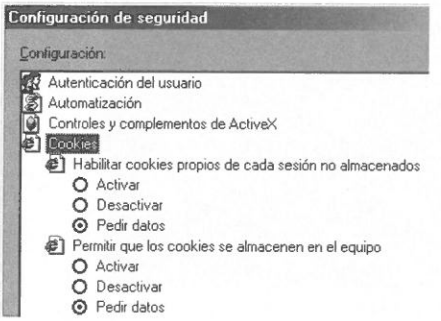
Navegador	Netscape Navigator	Internet Explorer
Cookie window title:	Netscape	Advertencia de seguridad
Expiration date text:	Es válido hasta	Válido hasta:
Cookie text:	Cookie	Cookie

Preparar correctamente los navegadores para Cookie Pal

Para que Cookie Pal pueda funcionar correctamente es imprescindible que el navegador web abra una ventana de advertencia cada vez que aparezca una cookie. Cookie Pal sólo se activa tras haber sido desplegada esta ventana, por lo que en caso contrario no funcionará. Durante la instalación, Cookie Pal realiza esta configuración automáticamente. Mientras no cambie nada en ella el programa funcionará a la perfección. Si no, siempre le quedará la opción de restaurar rápidamente las configuraciones necesarias.

Configurar Internet Explorer para Cookie Pal

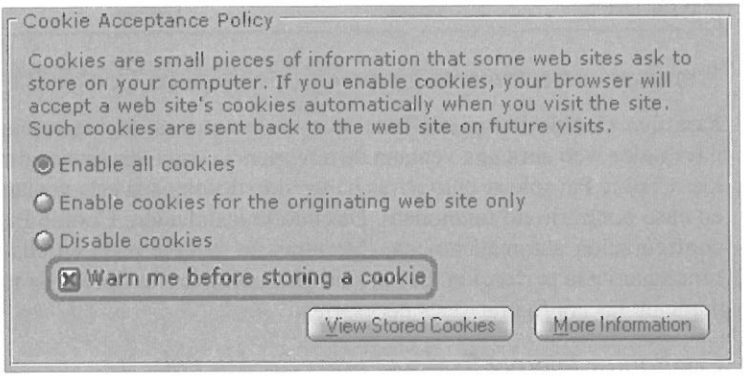
1. Acceda mediante *Herramientas/Opciones de Internet...* a la pestaña *Seguridad.*
2. Elija la zona de seguridad para la que desee cambiar las opciones de cookies. Si quiere ceder el manejo de las cookies totalmente a Cookie Pal, debería seguir los siguientes pasos para todas las zonas de seguridad y hacer clic sobre el botón de *Personalizar nivel.*
3. Busque en la lista de opciones de *Cookies* y active para ambas categorías la opción *Pedir datos*
4. Confirme las nuevas configuraciones dos veces con *Aceptar.*



Así configura usted Internet Explorer para Cookie Pal.

Configurar Netscape Navigator para Cookie Pal

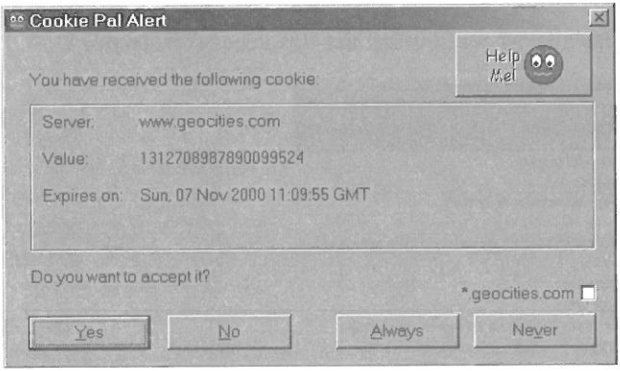
1. Seleccione *Edit/Preferences.*
2. Cambie a la categoría *Advanced.*
3. Active en el apartado *Cookies* la opción *Warn me before storing a cookie.*
4. Confirme el ajuste con *OK.*



Así configura usted Netscape Navigator para Cookie Pal.

Reaccionar con Cookie Pal ante las cookies

Cookie Pal viene configurado por omisión para que cuando aparezca una cookie emita una advertencia – de modo similar a lo que hace el navegador web – y deje la decisión al usuario. Pero, en comparación con los navegadores, Cookie Pal ofrece más posibilidades importantes para actuar.



Así advierte Cookie Pal de una cookie.

1. Primero, de forma similar a lo que hace Netscape Navigator, Cookie Pal da una información bastante exacta sobre el emisor (*Server*), el contenido (*Value*) y la vigencia (*Expires on*) de la cookie en cuestión.
2. Si usted lo quiere aceptar haga clic sobre el botón *Yes*. Con eso permitirá la consulta igual que ocurre en el navegador web.
3. Si, por el contrario, quiere rechazar la cookie, elija *No*. Tampoco aquí encontramos diferencias fundamentales con respecto a cualquiera de los navegadores web.
4. Si usted no sólo quiere aceptar esta cookie, sino también todos los demás que lleguen en el futuro desde ese ordenador, ya sea porque confía en el operador o por tratarse de una tienda virtual que no funciona sin cookies, haga clic sobre el botón *Always*.
5. Para rechazar la cookie y rehusar también todos las futuras cookies de esa máquina, porque usted no vea la necesidad de que esa página web deposite datos en su ordenador, haga clic sobre *Never*.
6. La opción situada encima de *Never* indica el dominio al que pertenece el servidor web que quiere colocar la cookie. Active esta opción antes de hacer clic sobre *Always* o *Never*, para que la decisión tomada no sólo actúe sobre este servidor concreto, sino también sobre todos los servidores de ese dominio.

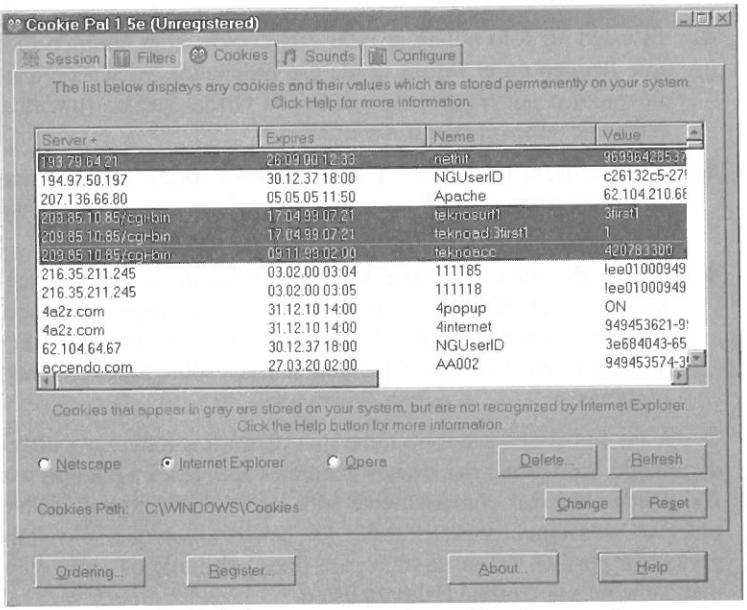
Con estas funciones usted no tiene que permitir o rechazar cada cookie individualmente, sino tomar decisiones generales aplicables a páginas web completas. Así puede autorizar cómodamente sólo las cookies imprescindibles, por ejemplo, para una tienda virtual. Todos los demás sitios que sólo empleen cookies para crear perfiles del visitante o para fines publicitarios serán rechazados automáticamente por Cookie Pal para usted.

Procesar las cookies

Con Cookie Pal usted no sólo puede reaccionar cuando entren cookies, sino también analizar y procesar los archivos de las cookies que se hayan acumulado en su PC. Esto permite visualizar las existencias de cookies y, si fuera necesario, limpiarlas concienzudamente. Le recomendamos que lo haga inmediatamente después de la instalación de Cookie Pal, para controlar no sólo las migajas de información nuevas, sino también las ya existentes.

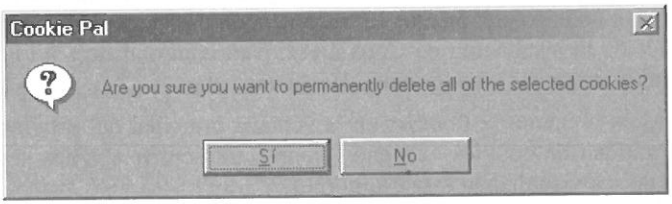
1. Abra la categoría *Cookies* en la ventana principal del programa. Según la cantidad de cookies existentes podrán transcurrir algunos segundos hasta que sea visualizada esta categoría.

2. A continuación, Cookie Pal listará las cookies almacenados hasta ahora en su PC por los navegadores.
3. Con las opciones *Netscape*, *Internet Explorer* y *Opera*, usted puede alternar entre las cookies de los diferentes navegadores.
4. Igual que en el Explorador de Windows puede marcar con el mouse las distintas entradas. En combinación con *[Mayús]* y *[Ctrl]* es posible seleccionar varias entradas a la vez.



Cookie Pal puede administrar y procesar las cookies almacenados.

5. Con el botón *Delete* usted borra de su ordenador las cookies seleccionadas. Para que ninguna cookie sea eliminada por accidente, se ha intercalado una consulta de seguridad. Confírmela con *Sí* para suprimir las cookies marcadas.



Confirme con Sí la consulta de seguridad.

Según la cantidad de cookies que se vayan a borrar, el proceso podrá llevar algún tiempo. Y es que Cookie Pal no se limita a borrar los datos, sino que actualiza simultáneamente el índice de cookies del navegador, para que éste refleje siempre la situación actual. Sólo así se pueden eliminar las cookies con seguridad, sin poner en peligro la estabilidad del navegador. Antes de borrarlas es conveniente cerrar el respectivo navegador web. De lo contrario, podría ocurrir que cookies recién borradas vuelvan a aparecer después.

8.3 Anónimo por la Red – navegar sin dejar huellas

Por desgracia el navegador web no es una calle de sentido único, por la que sólo le llega a usted información desde la Red y no al revés. El caso es más bien que los navegadores, debido al protocolo HTTP empleado, son bastante generosos en lo que respecta a la información sobre ellos mismos y sobre el propio ordenador y su usuario – es decir, usted.

INFO

¡Bienvenido, Klaus de Hamburgo!

¿Ha recibido usted alguna vez un saludo así de personal, al visitar una página web? Al principio, quizá pensó "¡Hombre, qué saludo tan majo!". Pero luego, igual se preguntó de dónde habría sacado el servidor web los datos personales necesarios para un saludo tan especial. Todos estos datos los puede obtener una página web consultando al navegador del usuario. Para entendernos: aquí no estamos hablando de pirateo, sino de funciones totalmente normales que son soportadas por los navegadores web modernos.

¿Qué información está en juego?

El protocolo HTTP prevé posibilidades con las que los servidores web pueden preguntar selectivamente determinados datos a un navegador web. La finalidad de todo esto es que el servidor web pueda ajustar sus páginas web con exactitud a las posibilidades de cada navegador. Por otro lado, ofrece a curiosos y hackers un buen punto de partida para espiar al visitante. Y es que de las respuestas que da el navegador a las consultas se pueden deducir multitud de informaciones:

- La dirección IP de su ordenador, de la que a su vez se puede derivar información sobre su proveedor de Internet.
- Según el caso, de lo anterior se desprenden también el lugar y el país de origen.
- El tipo de ordenador con el que usted se conecta a la Red.

- El sistema operativo con el que usted trabaja, de lo que por otra parte se deducen los agujeros de seguridad que pueda tener su ordenador.
- El navegador web que usted emplea, por lo que de nuevo se pueden averiguar agujeros de seguridad y puntos de partida para obtener más información.
- Su dirección de correo electrónico, si usted la tiene almacenada, por ejemplo, en el navegador web.
- Las aplicaciones que tenga instaladas en su PC.
- La última página web que visitó.
- La resolución de su monitor y el tamaño de la ventana del navegador.
- Si están permitidos los contenidos activos como Java, JavaScript o VBSript.

A partir de estos datos los hackers podrían deducir, por ejemplo, los métodos de ataque adecuados para espiar o sabotear a su PC. También los estrategas publicitarios podrían aprovechar esta información para hacerse una idea lo más exacta posible sobre los visitantes de sus páginas web.

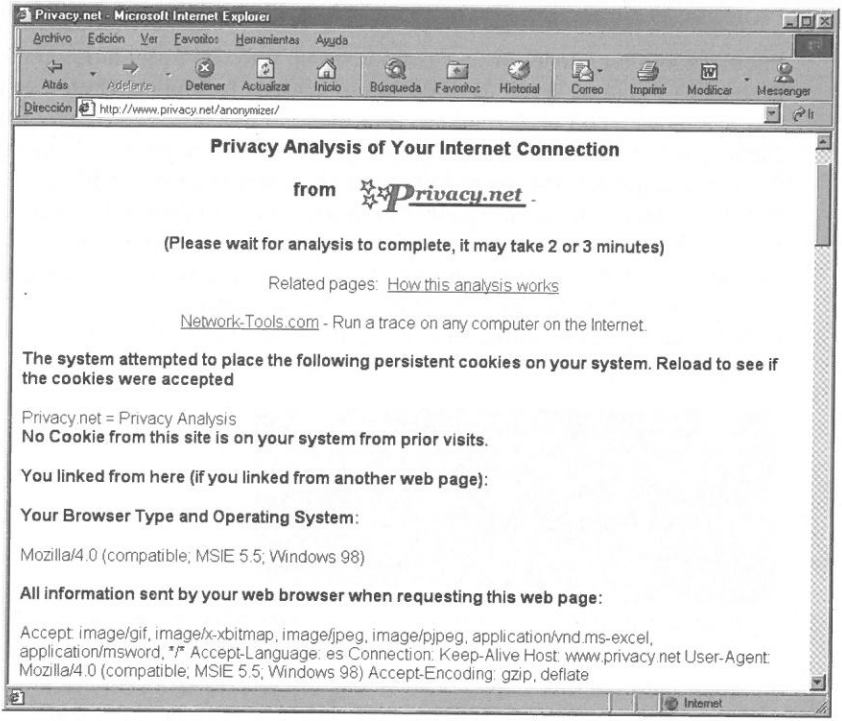
INFO

¿Cómo llegan los datos al servidor web?

Cada navegador web conoce determinados datos sobre sí mismo y su usuario, que transmite a los servidores web si estos se los piden. En algunos casos esta técnica tiene sentido. Los dos navegadores web más populares, Internet Explorer y Netscape Navigator, hoy en día ya se diferencian por muchos detalles de la representación de páginas. Por eso, para adaptar óptimamente las páginas web, muchos proveedores web preguntan primero con qué navegador trabajan sus visitantes, tras lo cual le transmiten una versión especializada de la página que solicitó. Aunque esta técnica en algunos ámbitos esté justificada, en conjunto ofrece un potencial innecesariamente grande para espiar información individual. Cada uno debe decidir por sí mismo, si desea facilitar a los proveedores datos demoscópicos tan importantes. Pero como muy tarde cuando alguien se dedique a sonsacar la dirección de correo electrónico, hay que cortar por lo sano. Porque entonces, los datos demoscópicos podrían ser asignados a personas concretas.

Haga la prueba: ¡Esto es lo que revela su navegador sobre usted!

La información exacta que sea revelada depende del navegador web y su configuración. Usted mismo puede hacer fácilmente la prueba para convencerse. En http://www.privacy.net/anonymizer encontrará una página web, que le muestra con exactitud toda la información sobre su ordenador que está al alcance de un servidor web.



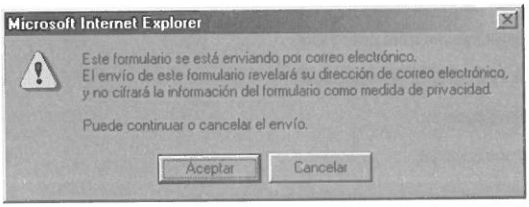
Haga la prueba: esto es lo que revela su navegador a servidores web "extraños".

Proteger con fiabilidad la propia dirección de correo electrónico

Un objeto de deseo especial son las direcciones de correo electrónico de los visitantes. Esto se debe a que, actualmente, las listas de direcciones electrónicas ya están tan comercializadas como las direcciones en la vida real. Si usted se pregunta ahora de dónde recibe constantemente publicidad por e-mail, aunque no haya revelado su dirección a nadie, la fuga de información quizá se deba a su navegador web. Por desgracia, tanto Internet Explorer como Netscape Navigator tienen agujeros de seguridad, que permiten a programadores web con ingenio averiguar las direcciones de correo electrónico de sus visitantes.

Proteger la dirección de correo electrónico en Internet Explorer

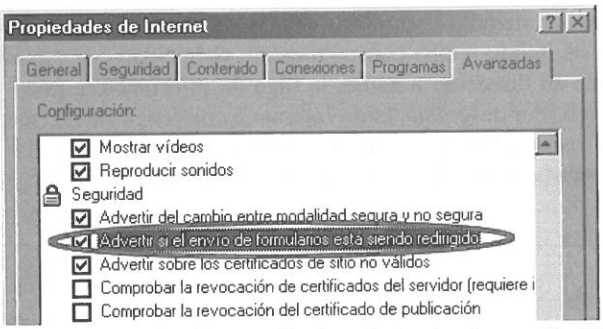
Internet Explorer puede ser persuadido con un truco de formulario relativamente sencillo, para que revele la dirección de correo electrónico. Basta con montar una página web con un formulario (por ejemplo una encuesta o un concurso) y hacer que el usuario remita los correspondientes datos por correo electrónico. Esto es una posibilidad del todo regular facilitada por los formularios HTML. Sólo que tontamente, el navegador web envía un e-mail donde figura como remitente la dirección de correo electrónico de su usuario. Con eso, el fisgón de datos ya puede vender una dirección más. Si al llamar a la página de análisis recibe una ventana de Internet Explorer que le advierte de este proceso, significará que el navegador ya está configurado con suficiente seguridad. En este caso podrá impedir con *Cancelar* que la dirección sea revelada.



Así le avisa a usted Internet Explorer de los intentos furtivos de averiguar su dirección de correo electrónico.

Si empleando Internet Explorer no se hubiera abierto esta ventana, le recomendamos que verifique urgentemente las configuraciones de seguridad.

1. Abra desde *Herramientas/Opciones de Internet...* la configuración de Internet Explorer.
2. pase a la pestaña *Avanzadas.*
3. Aquí encontrará en el apartado *Seguridad* la opción *Advertir si el envío de formularios está siendo redirigido.*



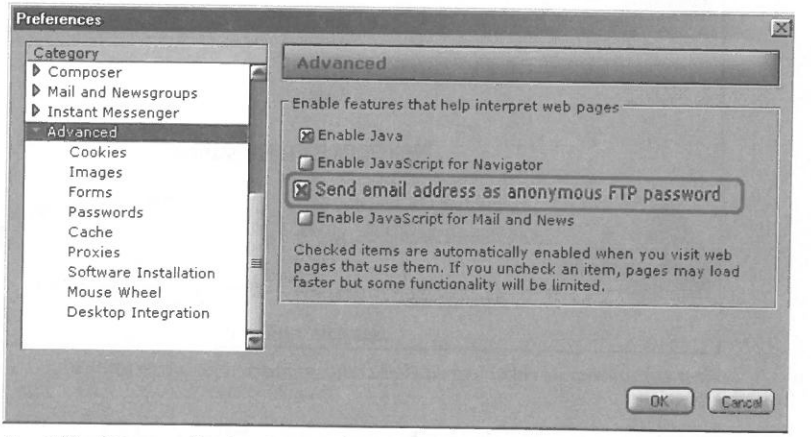
Así cierra usted en Internet Explorer la brecha de seguridad del e-mail.

4. Active esta opción para que, ante intentos de este tipo, el navegador dé la alarma y usted pueda impedir el proceso. Guarde las nuevas configuraciones con *Aceptar*.

Proteger la dirección de correo electrónico en Netscape Navigator

En Netscape Navigator el agujero del formulario está cerrado de fábrica pero, en su lugar, tiene otro que pueden aprovechar los cazadores de direcciones de e-mail que sean hábiles. El Navigator se puede registrar automáticamente en el FTP anónimo, indicando como contraseña la dirección de correo electrónico de usted, según exigen la mayoría de servidores FTP anónimos. También de esta función se puede abusar, fingiendo ante el navegador un inicio de sesión FTP anónimo para cazar la dirección de correo electrónico del usuario. Por eso, si usted no realiza regularmente un FTP anónimo, esta opción debería estar desconectada.

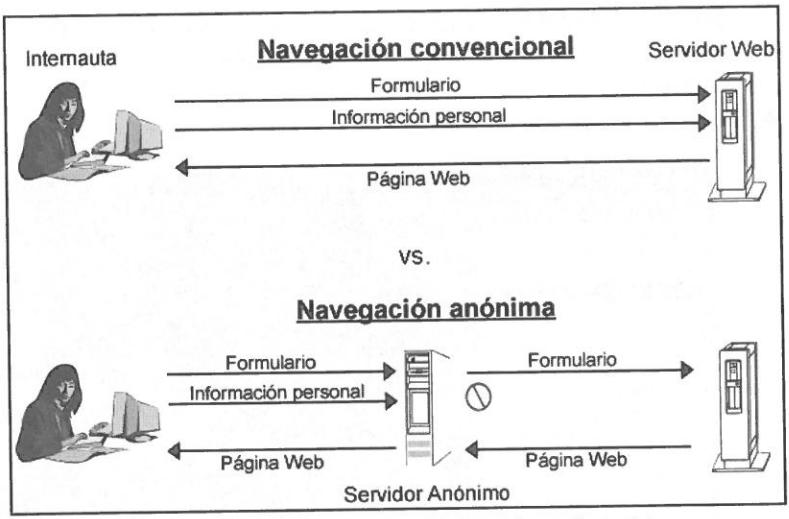
1. Abra con *Edit/Preferences* las opciones de Netscape Navigator.
2. Pase a la categoría *Advanced*.
3. Encontrará la opción *Send email address as anonymous FTP password*, que debería desactivar para cerrar este agujero de seguridad de Netscape Navigator.
4. Cierre las configuraciones después con *OK*.



También Netscape Navigator permite cerrar el agujero del e-mail con la opción correcta.

Así se hace: navegar de incógnito por la Red

Usted no tiene porqué aceptar pasivamente la curiosidad de los servidores web y la generosidad con que su navegador web reparte la información. Aunque no podamos convencer al navegador para que sea menos comunicativo, porque muchas de las funciones afectadas las exige el protocolo HTTP, hay servicios de Internet que realmente convierten en anónimas sus sesiones de navegación. En este caso usted no dirige sus consultas directamente al servidor web del que quiera obtener información. En lugar de eso recurre a un *Anonymizer*, un servidor web especial que recibe las consultas de usted y las remite al verdadero servidor. Durante este proceso el servidor del Anonymizer se presenta como navegador, es decir, el servidor al que usted se dirigía no podrá averiguar detalles sobre usted, el verdadero visitante. En lugar de eso el Anonymizer le despacha con informaciones vagas. Recibe las respuestas del servidor, es decir las páginas web, y se las transmite a usted. Como en ningún momento se produce un contacto directo entre su PC y el servidor web, éste tampoco podrá revelar ningún tipo de datos.



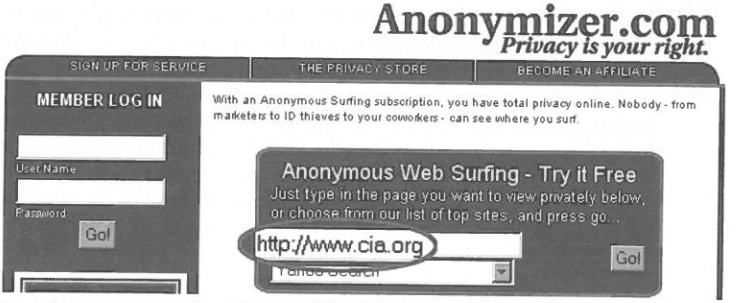
Para comparar: navegar por la Red como siempre y de modo anónimo.

Utilice un servicio de navegación anónimo

Encontrará un Anonymizer de este tipo bajo http://www.anonymizer.com. Los proveedores han detectado la necesidad de anonimato y la han convertido en un negocio. Por 5 $ al mes usted puede usar este servicio sin límite. Pero también hay disponible una versión gratuita, aunque deberá soportar en cada página web

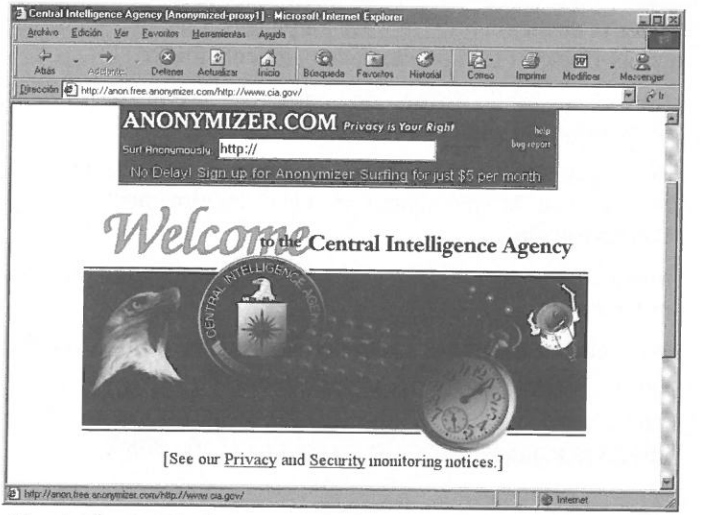
una pequeña pausa y la inserción de publicidad. No obstante, para probar este servicio o para navegar de vez en cuando anónimamente por la Red es suficiente.

1. Para solicitar páginas web anónimamente, basta con que en el navegador web introduzca http://www.anonymizer.com para llamar a la página inicial del servicio Anonymizer.
2. Teclee aquí la dirección deseada en el formulario *Surf Anonymously*.



Introduzca en el anonymizer la dirección que quiera visitar anónimamente.

3. Haga después clic sobre el botón *Go*.
4. Ahora, Anonymizer solicitará anónimamente la página deseada y la remitirá al navegador de usted. Éste visualizará la página, como si él mismo la hubiera descargado. Aunque en la variante gratuita de este servicio aparecerá en el margen superior el banner del Anonymizer.



Sin ningún tipo de riesgo: una breve visita anónima a la CIA..

5. A partir de ahora usted podrá seguir navegando anónimamente sin problemas. Anonymizer cambiará cada link en las páginas web transmitidas, para que sea llamado automáticamente en modo anónimo.

Sólo si usted introduce directamente una nueva dirección o llama alguno de los favoritos que tenga almacenados, dejará de navegar anónimamente.

TRUCO

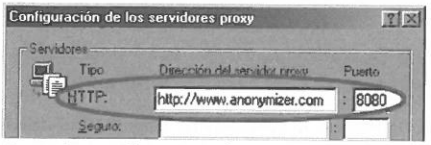
Sugerencia: introduzca la URL directamente

No es necesario que cada vez que usted quiera navegar anónimamente dé un rodeo a través de la homepage del Anonymizer. Si estructura bien la dirección web también podrá solicitar directamente las páginas web deseadas. Si usted quiere visitar la homepage de la CIA, en lugar de http://www.cia.gov debería teclear directamente http://www.anonymizer.com/http://www.cia.gov, para acceder a esa página de modo anónimo. Es decir, simplemente añada la dirección deseada a la dirección del servidor del Anonymizer. Con esto, también empleará el servicio de navegación anónimo, pero se ahorrará tener que llamar explícitamente a la página inicial.

Navegar siempre anónimamente – Ajustar Anonymizer como Proxy

¿Quizá usted quiera navegar siempre anónimamente por la Red? En ese caso, podrá evitarse el rodeo a través de la página inicial o la introducción de la dirección del Anonymizer. Este servicio de Internet también funciona como servidor Proxy, que puede recibir y procesar automáticamente todas las consultas de su navegador. Para eso usted sólo necesitará introducir en la configuración del navegador la dirección http://www.anonymizer.com:8080 como servidor Proxy. En Internet Explorer esto funciona del siguiente modo:

1. Abra el cuadro de diálogo de configuración con *Herramientas/Opciones de Internet...* y pase a la pestaña *Conexiones*.
2. En el apartado *Configuración de acceso telefónico*, elija la conexión de Internet con la que quiera navegar anónimamente y haga clic sobre *Configuración...*
3. Marque en el apartado *Servidor Proxy* la casilla de verificación *Usar servidor Proxy*.
4. Haga clic en *Avanzadas* para abrir la ventana *Configuración de los servidores Proxy*.
5. Ahora introduzca en la línea *HTTP* como dirección del servidor Proxy http://www.anonymizer.com y como conexión *8080*.



Introduzca el anonymizer como servidor proxy, para navegar siempre automáticamente de modo anónimo.

6. Confirme el ajuste del servidor Proxy con *Aceptar*.

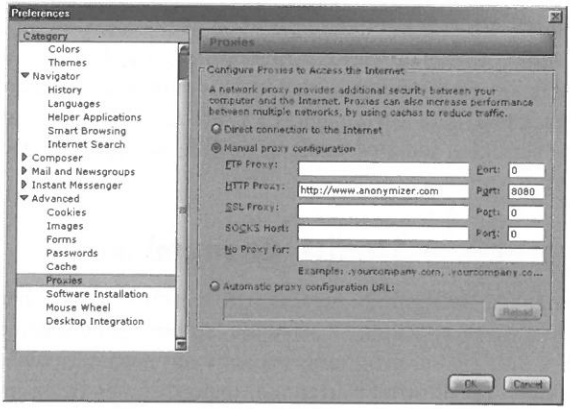
TRUCO

Conexión de Internet especial para navegar anónimamente

Con sus configuraciones flexibles de acceso telefónico, Internet Explorer también facilita la posibilidad de ajustar y usar una conexión de Internet especial para la navegación anónima. Usted sólo necesita copiar una de las conexiones telefónicas ya instaladas y darle a la copia otro nombre. Después, para esa nueva conexión telefónica establezca el Anonymizer como servidor Proxy, según hemos explicado anteriormente. Deje la otra conexión sin modificar. Ahora, desde el momento en que se conecte a Internet, podrá decidir con la elección de la conexión telefónica correspondiente, si quiere navegar a cara descubierta o prefiere hacerlo anónimamente.

También en Netscape Navigator se puede definir un Anonymizer como Proxy.

1. Abra con *Edit/Preferences* las opciones de Netscape Navigator.
2. Cambie ahora a la categoría *Advanced* y desde allí, a la subcategoría *Proxies*.
3. Active ahora la opción *Manual proxy configuration*.
4. A continuación introduzca en el campo *HTTP-Proxy* la dirección del Anonymizer http://www.anonymizer.com y detrás de ésta, en el campo *Port*, el número de puerto *8080*.



También Netscape Navigator permite ajustar el Anonymizer como servidor Proxy.

5. Guarde la nueva configuración de Proxy con *OK*.

Desgraciadamente Netscape no permite ajustar el Proxy para cada conexión, por lo que este sistema deberá aplicarse siempre de modo general.

A partir de ahora todas las consultas a la Red serán tramitadas automáticamente a través del servicio Anonymizer. Aunque si usted emplea varias conexiones a Internet, debería cambiar todas del modo descrito. Si su proveedor exige que indique un servidor Proxy propio, este procedimiento no servirá para ese acceso. Pero en ese caso, usted quizá pueda recurrir a un software Anonymizer especial, como el que vamos a presentar en el siguiente apartado.

Para los que quieran estar muy seguros: el software Anonymizer

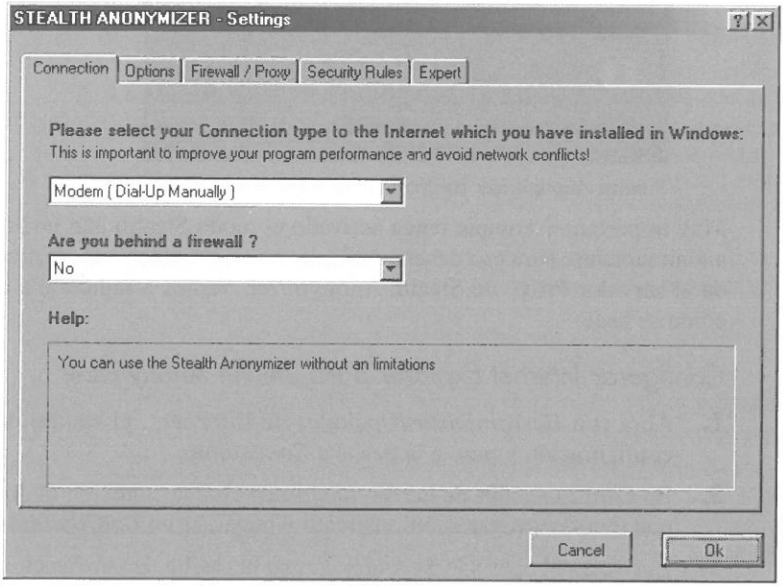
Para que usted pueda navegar por Internet bajo un anonimato tan fiable como confortable, queremos concluir ese capítulo presentándole un software que permite justamente eso. *Stealth Anonymizer* es conectado como servidor Proxy local entre su PC e Internet. Usted puede descargar una versión gratuita en http://www.photono-software.de. Stealth Anonymizer domina varios modos de operación y usted podrá pasar de uno a otro siempre que lo necesite.

- En el modo *DirectNet*, el programa establece directamente todas las conexiones, es decir, no crea ningún anonimato. A cambio de eso la navegación se desarrolla a la velocidad habitual.
- En el modo *Stealth*, el programa camufla las actividades de usted dirigiéndolas a través de uno de varios servidores Anonymizer. Para cada nueva conexión cambia de servidor, de modo que difícilmente le podrán seguir a usted la pista.
- Además, para los clientes registrados existe también la modalidad *SUPERStealth*. En este modo de operación cada conexión de datos es dirigida enseguida a través de varios Anonymizer en todo el mundo. También esta combinación de diferentes estaciones es cambiada constantemente. De esta manera hasta para los cazadores profesionales de datos, como por ejemplo los servicios secretos, sería imposible averiguar la procedencia de una consulta.

Instalar y preparar Stealth Anonymizer

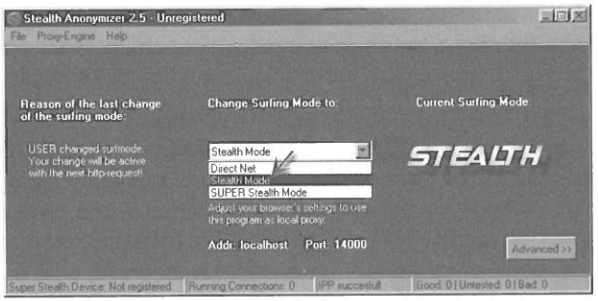
Stealth Anonymizer es configurado mediante un asistente y no es necesario tener en cuenta ningún paso en especial. El asistente también genera una entrada en la carpeta de Inicio, para que el programa sea activado automáticamente cada vez que inicie Windows. En el primer arranque, justo después de la instalación, se abrirá automáticamente el menú de configuración, donde usted deberá introducir dos parámetros importantes.

1. En el campo de selección del margen superior *Please select your Connection type to the Internet which you have installed in Windows*, indique cómo establece su PC la conexión con Internet. Si usted se conecta siempre manualmente elija la opción *Modem (Dial-Up Manually)*. Si, cuando lo necesita, su PC establece automáticamente la conexión telefónica vía módem (o también RSDI), seleccione la opción *Modem (Dial-Up On Demand)*. Si usted no emplea módem ni adaptador RSDI y su PC está conectado a Internet a través de una red, convendrá usar las opciones *LAN*. Aquí aún habrá que elegir entre una conexión permanente (Permanent Online) y una conexión bajo demanda *(Dial-Up On Demand)*.
2. Además, en el campo de selección *Are you behind a firewall?*, usted deberá indicar si su PC está protegido ante Internet mediante firewall. Pero por esto no se entiende un firewall personal como los que presentamos en el Capítulo 4, sino soluciones profesionales que blindan redes enteras. Si éste es su caso, por ejemplo en un ordenador de empresa, elija la opción *Yes*. Aunque aquí, deberá realizar más configuraciones en la categoría *Firewall / Proxy*. Los datos que necesite debería preguntárselos a su administrador de redes. Si su PC no posee una protección por firewall seleccione la opción *No*. En este supuesto, podrá usar Stealth Anonymizer sin necesidad de tomar más medidas.



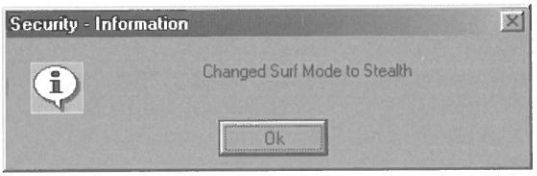
La primera vez que arranque Stealth Anonymizer deberá realizar algunos ajustes importantes.

3. A continuación haga clic sobre *OK* para aceptar y guardar las configuraciones.
4. Ahora pasará a la ventana principal de Stealth *Anonymizer*, donde podrá elegir en el campo de selección central el modo de operación con el que quiera navegar.



En la ventana principal de Stealth Anonymizer puede elegir el modo de navegación.

5. En función del modo de operación elegido recibirá ahora la confirmación del cambio, que deberá cerrar haciendo clic sobre *OK*.

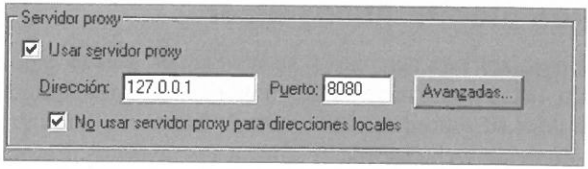


Stealth Anonymizer confirma el cambio al modo Stealth.

Muy importante: Aunque tenga activado el modo Stealth aún no podrá navegar anónimamente. Para eso deberá configurar su navegador web de modo que acceda al servidor Proxy de Stealth Anonymizer. Vamos a indicarle a continuación cómo se hace.

Configurar Internet Explorer para Stealth Anonymizer

1. Abra con *Herramientas/Opciones de Internet...* el cuadro de diálogo de configuración y pase a la pestaña *Conexiones*.
2. En *Configuración de acceso telefónico* elija la conexión de Internet con la que quiera navegar anónimamente y haga clic en *Configuración...*
3. Active en el apartado *Servidor Proxy* la casilla de verificación *Usar servidor Proxy*.
4. Introduzca como *Dirección* del servidor Proxy *127.0.0.1* y como *Conexión* el número *14000*.

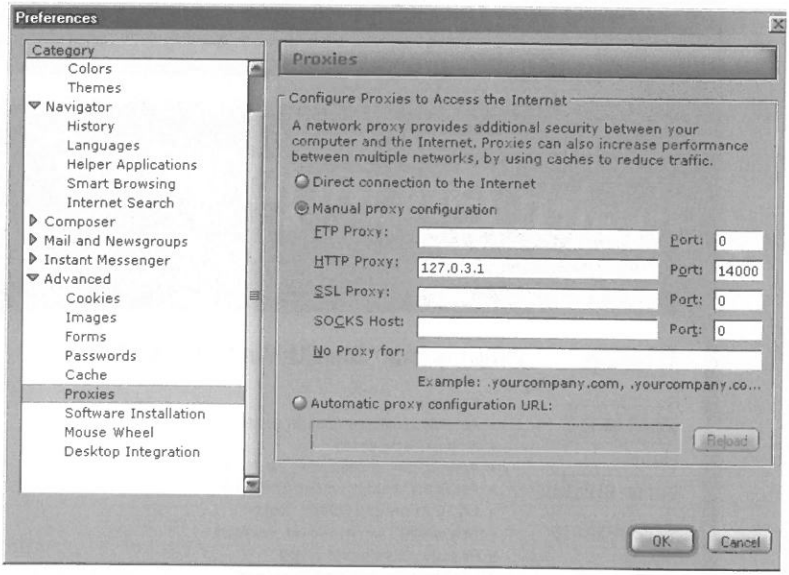


Introduzca Anonymizer como servidor Proxy, para navegar siempre automáticamente en modo anónimo.

5. Cierre ahora con *Aceptar* todas las ventanas de menú abiertas.

También Netscape Navigator debe ser configurado para el trabajo conjunto con Stealth Anonymizer.

1. Abra con *Edit/Preferences* las opciones de Netscape Navigator.
2. Cambie a la categoría *Advanced* y, desde allí, a la subcategoría *Proxies.*
3. Active aquí la opción *Manual proxy configuration.*
4. Introduzca en el campo *HTTP-Proxy* el número IP *127.0.0.1* y detrás, en el campo *Port*, el número de puerto *14000.*



También en Netscape Navigator se puede ajustar el anonymizer como servidor proxy.

5. Guarde con *OK* la nueva configuración de Proxy.

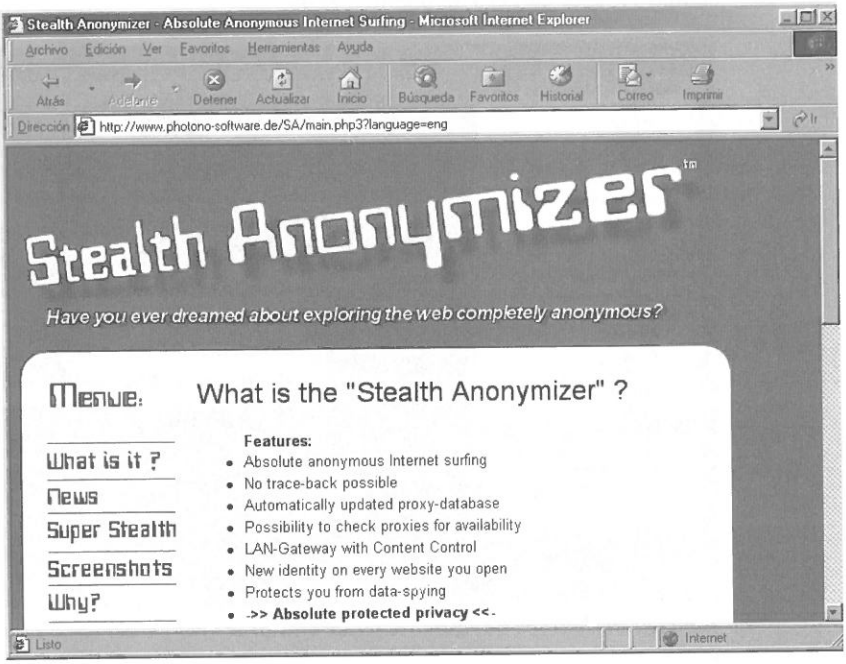
Navegar con Stealth Anonymizer

Si Stealth Anonymizer está activado y su navegador web ha sido configurado como es debido, usted podrá navegar alegremente por donde quiera. Ni siquiera tendrá que cambiar su procedimiento habitual. Basta con que introduzca en el navegador la dirección web deseada, o llame a sus favoritos. En primer lugar, el navegador enviará todas sus consultas a Stealth Anonymizer. Este las convertirá en anónimas (¡siempre que el modo Stealth esté conectado!) y las remitirá al verdadero servidor web. Después esperará la respuesta, la recibirá y la pondrá a disposición de su navegador web, que la visualizará como de costumbre.

TRUCO

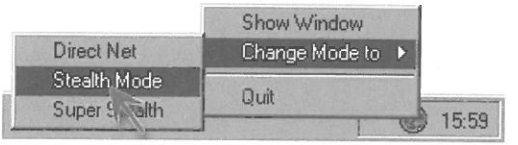
Probar Stealth Anonymizer

Para probar su buen funcionamiento puede descargarse una página de evaluación de la página web del fabricante. Ésta indica la dirección IP del ordenador desde el que fue solicitada. Si usted la llama o actualiza repetidamente, cada vez debería aparecer un número IP diferente, en cuyo caso Stealth Anonymizer estaría trabajando correctamente. De lo contrario verifique si fue activado el modo Stealth realmente y si el navegador web está bien configurado.



Con la página de test usted puede verificar el funcionamiento de Stealth Anonymizer.

Para cambiar el modo de operación del programa usted puede hacer en todo momento doble clic en el icono de Stealth Anonymizer situado abajo a la derecha, en la Barra de tareas. Esto abrirá la ventana principal, con el campo de selección ya conocido. Aún podrá ir más deprisa con el menú contextual. Para abrirlo basta con hacer clic sobre el icono con el botón derecho del mouse. Bajo *Change Mode* encontrará un submenú con los modos de operación ya conocidos. Por favor, tenga en cuenta que el modo *Super Stealth* sólo funciona en la versión de pago registrada del programa.



A través del menú contextual puede cambiar rápidamente y en cualquier momento el modo de navegación.

9. Proteger las páginas de inicio contra los hackers

9.1 ¿Qué revela sobre usted su propia página web? 499
Registrar y analizar las páginas web 499
Proteger las páginas web contra los ladrones de información 506
Impedir el uso fraudulento de las imágenes publicadas 510
9.2 Páginas web manipuladas 511
Proteger las páginas web contra los ataques 512
9.3 Contraseñas, archivos y áreas protegidas 514
9.4 Posibilidades de ataque sobre servidores web 516

Si usted no se limita a navegar por la Red, sino que también ofrece su propia información en la misma, por ejemplo mediante una página web personal, se expone a peligros adicionales. Según el lema "todo lo que diga podrá ser utilizado en su contra", saboteadores malévolos o bromistas con un sentido del humor retorcido, podrían emplear contra usted sus propias páginas web. Aquí, en principio distinguimos dos tipos de peligros:

- Los hackers pueden analizar el contenido de sus páginas para obtener información que les serviría a la hora de lanzar ataques contra usted, o
- los hackers pueden cambiar el contenido de las propias páginas web, poniendo así en boca de usted declaraciones que nunca hizo.

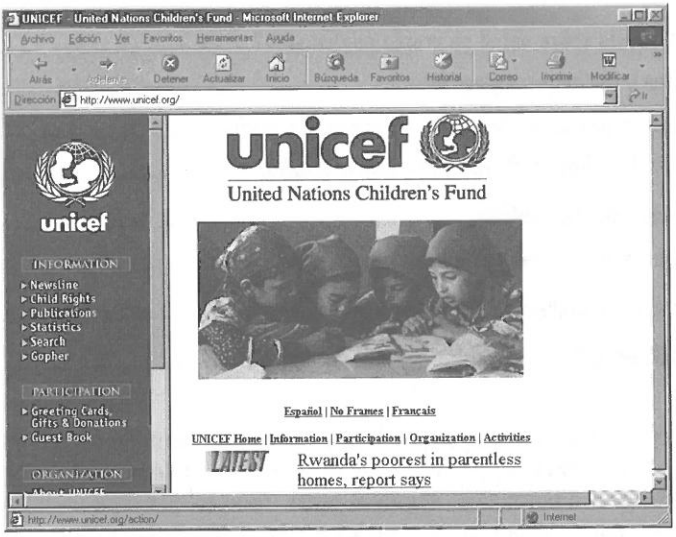
En este capítulo vamos a ocuparnos de los agujeros de seguridad que surgen al ofrecer información en Internet y de cómo resolverlos.

INFO

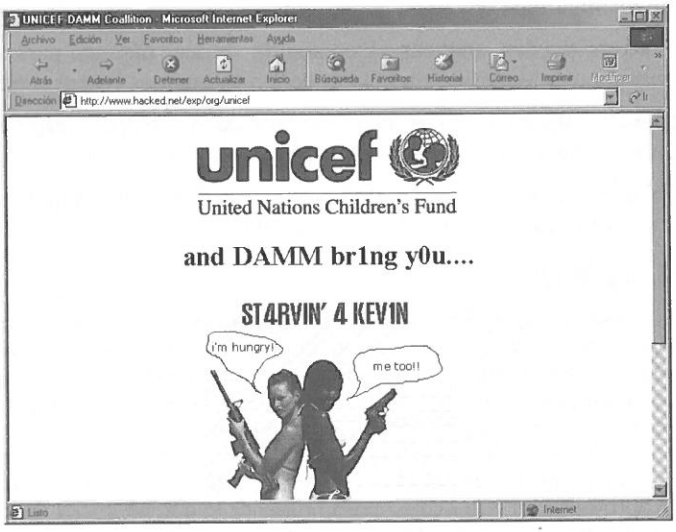
El pirateo a UNICEF

En los últimos años, los hackers han atraído la atención una y otra vez por sus espectaculares ataques de rediseño. Este tipo de agresiones se dirigen a páginas web importantes y muy visitadas, transformando su apariencia para que reproduzcan un mensaje de los hackers. Uno de los más notorios fue el perpetrado contra la página web de la institución benéfica de ayuda a la infancia de las Naciones Unidas (UNICEF). Los hackers averiguaron la contraseña con la que los empleados de UNICEF accedían al servidor web. Luego aprovecharon este acceso para rediseñar la página inicial de la web de UNICEF, colocando un manifiesto con el que exigían la liberación de su colega Kevin Mitnick, encarcelado por entonces. Transcurrieron algunas

horas hasta que UNICEF se percató del suceso y pudo restablecer la página. Este tiempo bastó para que muchos visitantes advirtieran el ataque y éste alcanzara gran repercusión en los medios de comunicación. Podrá encontrar una recopilación de ataques por rediseño que tuvieron éxito en la dirección: http://www.hacked.net.



Este era el aspecto original de la página web de UNICEF.



Esta es la versión que dejaron los hackers tras su ataque.

9.1 ¿Qué revela sobre usted su propia página web?

Casi siempre, las páginas web, especialmente las páginas personales, revelan algunas cosillas sobre su propietario. Todo el mundo quiere transmitir en ellas una imagen lo más completa posible acerca de sí mismo, por lo que escribe de todo sobre su persona, aficiones e intereses, publicando casi siempre hasta alguna que otra foto suya y de sus amores. Pero todos estos datos también pueden volverse contra su autor si, por ejemplo, sirven a los hackers como fuente de información para hacer social hacking (vea el Capítulo 1).

Pero también hay otros que recurren de buen grado a los datos que usted mismo facilita con tanta alegría. En la industria informática, por ejemplo, hoy en día es del todo habitual que a la hora de procesar las solicitudes de empleo las empresas investiguen en Internet sobre los candidatos. Esto, en principio, no es malo. A fin de cuentas, la información está al alcance de todos. Pero si la empresa da con declaraciones que contradigan lo que usted puso en su solicitud, las oportunidades se le esfumarán, y esto puede ocurrir con demasiada facilidad. Porque hay ciertas cosas, por ejemplo opiniones políticas o aficiones personales, que no se suelen mencionar en una solicitud de trabajo. Pero si usted hace proselitismo de ellas en su homepage u ofrece vínculos a otras páginas web relacionadas con estos temas, el que podría ser su futuro jefe las conocerá de todos modos.

Por último, los coleccionistas de datos profesionales sacan provecho de las páginas personales. En casi todas estas páginas figura, por ejemplo, la dirección de correo electrónico del autor. Hoy en día, estas direcciones son una mercancía comercial altamente codiciada por las empresas de marketing. Con la ayuda de mecanismos de búsqueda automatizados, como los que se emplean en los buscadores, es posible recopilar, a gran escala y de modo totalmente automático, las direcciones de e-mail publicadas en homepages, para analizarlas después.

Registrar y analizar las páginas web

Teniendo en cuenta la enorme extensión de Internet y la ingente cantidad de páginas web (según estimaciones prudentes, su número ya ronda el límite de los mil millones), de momento da la impresión que va a ser imposible encontrar detalles de información tan personales. Pero, según hemos explicado en el capítulo precedente, recurriendo a los buscadores no es tan difícil recopilar información acerca de determinados individuos. Además, generalmente nadie oculta las páginas privadas. Al contrario, se suele llamar la atención sobre ellas para atraer el máximo número de visitantes posible, y una vez hallada la dirección que corresponda a la homepage de la persona buscada, es muy fácil analizarla. Herramientas especiales, como pueden ser los navegadores offline, permiten

copiar al propio ordenador el contenido completo de una página web, para analizarla exhaustivamente. Un instrumento que resulta muy práctico para este propósito es *Teleport Pro*, del cual se puede descargar una versión de prueba en la dirección http://www.tenmax.com. Teleport Pro es capaz de bajarse páginas web completas para someterlas a un análisis offline o sin conexión. Aparte de esto, el programa ofrece funciones específicas que resultan indicadas, sobre todo, para realizar pesquisas. Por ejemplo, la exploración selectiva de las distintas páginas de una página web en busca de determinadas palabras clave. Quizá sería recomendable que usted sometiera a su propia página web a un análisis con Teleport Pro, para comprobar toda la información que alguien pudiera obtener sobre usted a partir de la misma. En las siguientes páginas, vamos a mostrarle cómo se hace.

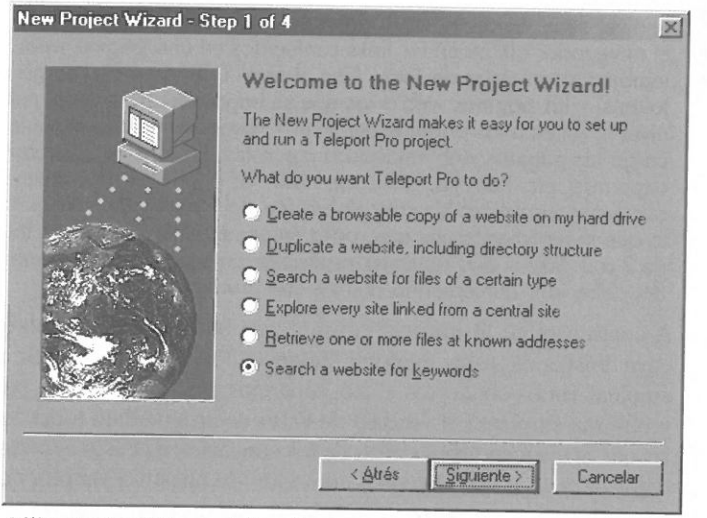
Registrar y analizar páginas web con Teleport Pro

Teleport Pro es un navegador offline, es decir, según las instrucciones que usted le dé, navegando puede "pescar" automáticamente páginas web completas y almacenar localmente en su disco duro los datos recopilados. Después, estos datos podrán ser contemplados offline con toda tranquilidad, sin que el contador de tarifas esté haciendo tictac. Además, las copias de las páginas web almacenadas localmente pueden ser analizadas mejor que si hay que descargarlas cada vez del servidor. Todo lo que usted necesita para usar Teleport Pro es la dirección web en la cual esté alojada la página, es decir, simplemente la dirección que usted introduciría en el navegador web.

1. Cuando inicie Teleport Pro por primera vez, se arrancará automáticamente el asistente de proyectos, con el que podrá dar de alta nuevos proyectos. Teleport Pro entiende por proyecto todos los datos sobre el sitio web que deba captar, al igual que las páginas obtenidas después de ese sitio web. También es posible iniciar el asistente más tarde, si utiliza la función de menú *File/New Project Wizard...*

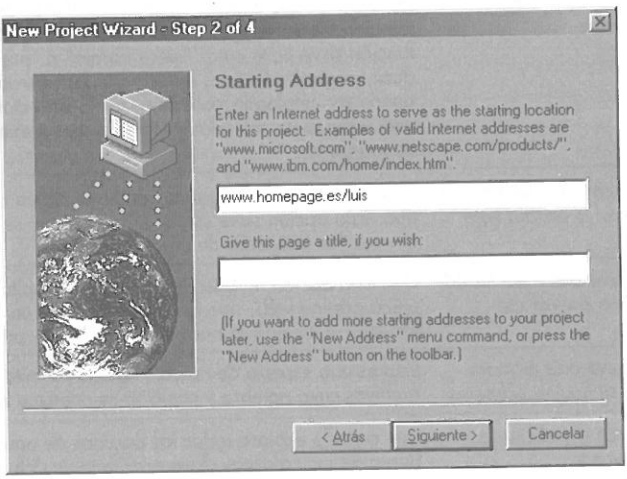
2. En el primer paso del asistente, seleccione el tipo de proyecto y decida cómo deberá solicitar Teleport Pro las páginas web y hasta qué límite (vea la tabla). Para buscar información de forma selectiva, resulta especialmente indicada la última opción *Search a website for keywords*. Si, por el contrario, lo que se desea es recoger toda una página web, habría que seleccionar la opción *Create a browsable copy of a website on my hard drive.*

Tipo de proyecto	Significado
Create a browsable copy of a website on my hard drive	Teleport Pro genera en el disco duro una copia del sitio web, que podrá ver en el navegador como si estuviera online y solicitara las páginas directamente al servidor.
Duplicate a website, including directory structure	El programa genera en el disco duro una copia exacta de los archivos que componen el sitio web, teniendo en cuenta también las estructuras de directorios. En realidad, esta función sirve para crear "sitios espejo" o "mirrors", es decir, páginas idénticas en un servidor alternativo. También puede ser empleada para analizar la estructura de un sitio web y quizá los métodos y técnicas que prefiera el autor de la misma.
Search a website for files of a certain type	Únicamente se descargan los archivos de un determinado tipo. Esta opción sirve si, por ejemplo, sólo se quieren obtener las imágenes de un sitio web.
Explore every site linked from a central site	Con esta opción, la búsqueda no queda limitada a una única página web, sino que también tiene en cuenta todos los sitios a los que se hace referencia en la página inicial.
Retrieve one or more files at known adresses	Esto es una especie de modo FTP, que permite descargar archivos cuyo nombre y posición se conozca con exactitud.
Search a website for keywords.	Este método explora todas las páginas de una web, en busca de las palabras clave previamente definidas. Registra todas las páginas que las contengan. Esta función tiene especial interés para realizar indagaciones.



Elija en primer lugar el tipo de proyecto.

3. En el segundo paso, indique la dirección bajo la cual Teleport Pro deba buscar una página web. Emplee la URL de inicio, que también introduciría en el navegador web si quisiera visitar ese sitio. Establezca, además, con *Up to X links from starting point* el nivel de inclusión que deba emplear el programa.



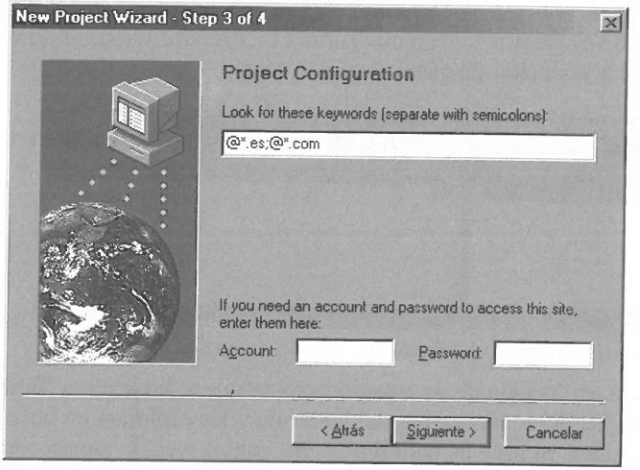
Introduzca la dirección inicial de la oferta web que quiera guardar.

TRUCO

El nivel de inclusión correcto

El nivel de inclusión indica cuántas veces deberá entrar, durante la descarga, el navegador offline en los links contenidos en una página web, para bajarse también las páginas de éstos. Con el nivel 1, Teleport Pro carga el documento en sí y las páginas web a las que se haga referencia en el mismo. En el nivel 2, analiza las páginas del nivel 1 cargadas adicionalmente y también carga las páginas web enlazadas con éstas. En el nivel 3, profundiza una capa más, etc. Por ello, con cada nivel, las páginas a transmitir pueden aumentar considerablemente en función del número de links contenidos. Por lo que le recomendamos que, para empezar, elija un nivel de inclusión bajo, de 2 a 3. Sólo si esto resultara insuficiente para obtener la información deseada, debería ir aumentando el nivel con prudencia.

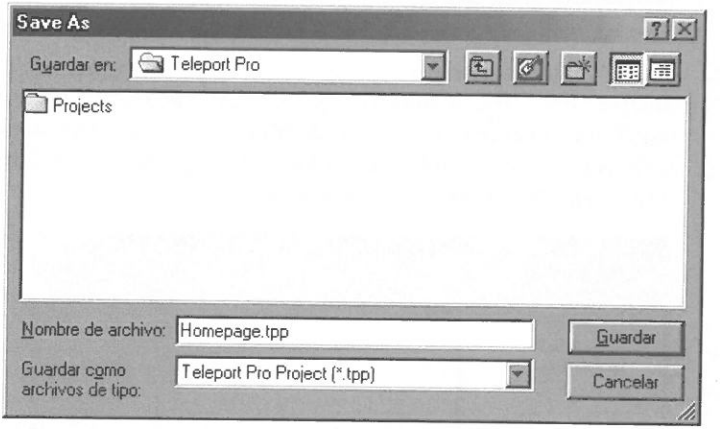
4. A continuación, formule el concepto de búsqueda o las palabras clave en cuya búsqueda deba explorar Teleport Pro las páginas. Si usted quiere emplear varios conceptos clave, sepárelos con una coma (,), para lo cual, el programa empleará el vínculo de O, es decir, guardará todas las páginas en las que aparezcan uno o varios de los conceptos de búsqueda. Además, podrá emplear el asterisco (*) como comodín. En nuestro ejemplo, queremos buscar direcciones de correo electrónico, por lo que empleamos las palabras clave *@*.es* y *@*.com*, para dar con todas las direcciones ES y COM.



Introduzca las palabras clave que deba buscar Teleport Pro en las páginas web.

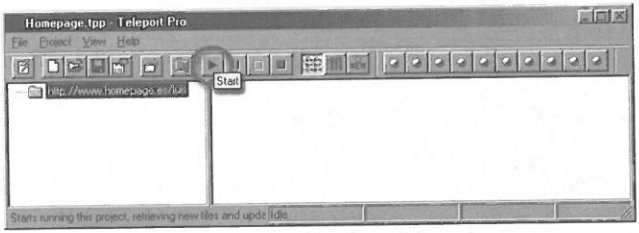
5. Con esto concluye la configuración del proyecto. Haciendo clic sobre el botón *Finalizar* cerrará el asistente.

6. Ahora habrá que almacenar el proyecto recién creado. Para eso, Teleport Pro abre automáticamente un cuadro de diálogo denominado *Save as*, donde usted deberá seleccionar una carpeta e indicar el nombre de archivo a guardar. El programa propone automáticamente un nombre, basándose en la dirección del sitio web; así puede aceptar esa sugerencia, si lo desea, o modificarla.



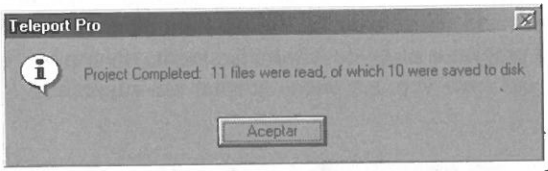
Almacene el nuevo proyecto en un archivo.

7. Ya puede solicitar la ejecución del proyecto. Para tal fin, selecciónelo en la lista de proyectos y haga clic sobre el icono *Start* de la barra de iconos, o llame a la opción de menú *Project/Start*.



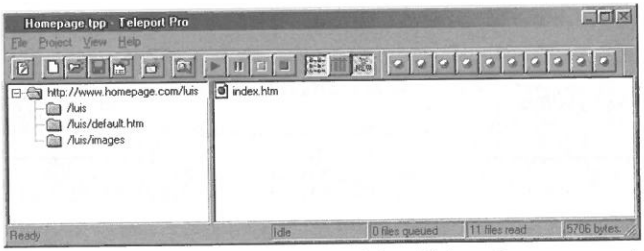
Ejecute el proyecto haciendo clic sobre el icono de arranque.

8. Ahora, en función de las especificaciones que usted le diera, Teleport Pro solicitará las diferente páginas del homesite y las explorará en busca de las palabras clave. Si hace un hallazgo en una página web, la almacenará y proseguirá la búsqueda hasta que haya explorado todas las páginas (dependiendo del nivel de inclusión). A continuación, mostrará un breve resumen del proyecto, donde podrá ver el número de páginas que fueron analizadas y cuántas de ellas se almacenaron localmente. Cierre la ventana de estado haciendo clic sobre *Aceptar*, para volver a la ventana principal de Teleport Pro.



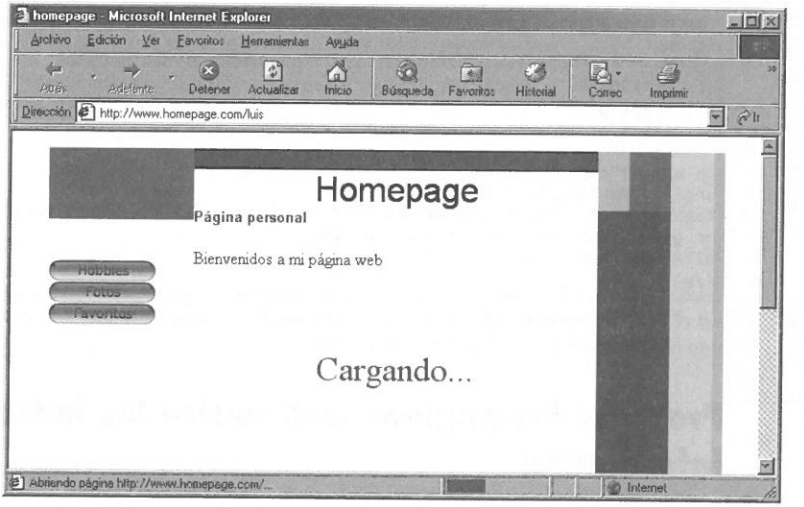
Una vez finalizado el análisis, Teleport Pro muestra un breve resumen.

9. En la ventana principal, podrá ver ahora la información obtenida por Teleport Pro sobre el sitio web que se quería analizar. En la ventana de la izquierda, encontrará un cuadro de conjunto con la estructura de la página web. A la derecha aparecerán siempre las páginas o los archivos que contengan uno de los conceptos de búsqueda.



Teleport Pro muestra los resultados del análisis en la ventana principal.

10. Si quiere ver la página web, basta con hacer doble clic sobre la entrada correspondiente. Teleport Pro arrancará el navegador web y mostrará el archivo a través de éste.

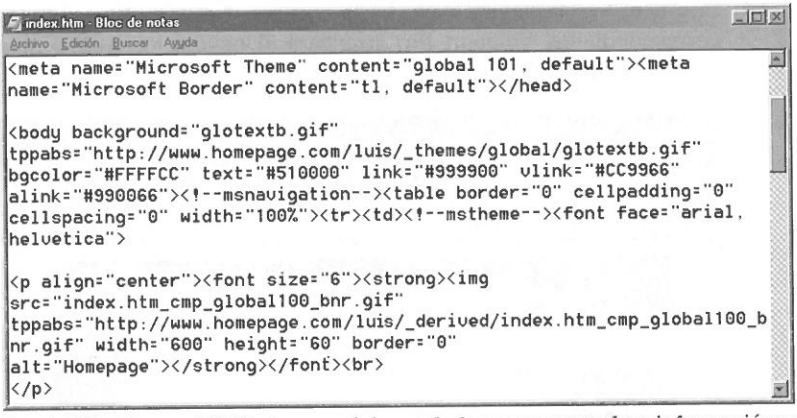


Con un doble clic puede solicitar y ver las páginas web almacenadas localmente.

TRUCO

Palabras clave en el código fuente

Trabajando con Teleport Pro le ocurrirá con frecuencia, que en una página web almacenada localmente no encuentre las palabras clave que realmente buscaba. Esto se debe a que el programa no sólo explora el contenido de las páginas web, sino también todo el código. Éste podrá contener mucha información, que en realidad no sea visible en la página verdadera. Esto ocurre sobre todo con direcciones, pero también con textos que puedan haber sido incluidos en el texto fuente como comentarios. En estos casos, no debería observar sólo la página en sí, sino también el texto fuente o código. Emplee para ello la correspondiente función de su navegador web, o llame de entrada a la página en código fuente html desde la ventana principal de Teleport Pro, haciendo clic sobre su entrada con la tecla derecha del mouse y seleccionando la función *Edit* en el menú contextual. Eso hará que el código de la página se muestre en un editor de textos.



En el código fuente HTML de una página web, frecuentemente hay información que uno no encuentra en la página verdadera.

Proteger las páginas web contra los ladrones de información

¿Puede protegerse de esta clase de espionaje quien publique páginas web? Las medidas de protección técnicas, como por ejemplo la encriptación de páginas web, fracasan por el principio básico de la Red. A fin de cuentas, ésta vive de que los datos publicados estén al alcance de todo el mundo con absoluta libertad. Aun así, hay estrategias para controlar la información personal revelada en las páginas web.

¿Qué información revela usted?

En primer lugar, debería plantearse qué información personal desea revelar a otros. Estudie para ello su página y analice qué conclusiones permite sacar sobre su persona, ya sea directa o indirectamente, la información contenida en la misma. Piense en cada asunto si éste podría ser empleado contra usted. En función de cómo sean sus tendencias a la paranoia, la lista podrá ser más o menos larga. El lugar de residencia y la dirección figuran en relativamente pocas homepages. Parece que la mayoría de la gente tiene claro que esta información debe ser protegida contra fisgones y acosadores. Pero si figuran la fecha y el lugar de nacimiento, un espía que disponga de los recursos adecuados también podría dar con la pista correcta, ya que casi siempre se puede seguir el rastro de una persona desde su lugar de nacimiento hasta su domicilio actual. Los organismos estatales de investigación o los servicios secretos sólo precisan una breve consulta a las bases de datos para hacerlo. Los fisgones particulares necesitarán algo más de paciencia y quizá, algún soborno.

También habría que preocuparse un poco de la dirección virtual. En principio, no hay nada que objetar a que una dirección de correo electrónico pueda ser consultada por todo el mundo, como sucede con un número de teléfono. Pero si usted ya ha tenido experiencias desagradables o teme que las pueda tener, debería renunciar a convertir su dirección de correo en un bien común. La solución es muy sencilla: recurra a alguna de las muchas páginas de correo web gratuitas y hágase así con una dirección para publicarla en las páginas web. Por ejemplo, podría solicitar que redireccionen los mensajes recibidos a su dirección de correo normal, sin que los remitentes lo sepan. Esto ofrece la ventaja de que la dirección no conduce directamente hasta usted. Además, en un caso de apuro siempre podrá cancelar esa dirección y sustituirla por otra; por ejemplo, si le molestaran vía e-mail o le llenaran la bandeja de correo spam o basura. (Hay más sugerencias sobre este tema en el Capítulo 7).

Este principio puede ser ampliado a voluntad. Supongamos que usted tiene un hobby secreto o defiende alguna idea religiosa o política, que no deban conocer su jefe o algún compañero de trabajo curioso. Esto no significa que deba renunciar a crear una página web sobre ese tema. Intente simplemente separar esa página de su persona, adoptando una identidad virtual que no permita sacar conclusiones sobre su identidad real. Las direcciones de correo electrónica gratuitas y las ofertas de espacio libre en la Red resultan idóneas para este propósito. Así, podrá disfrutar bajo un seudónimo o un alias de sus pasiones privadas, sin temor a que husmeadores entrometidos descubran su secreto.

Tapar agujeros de información innecesarios

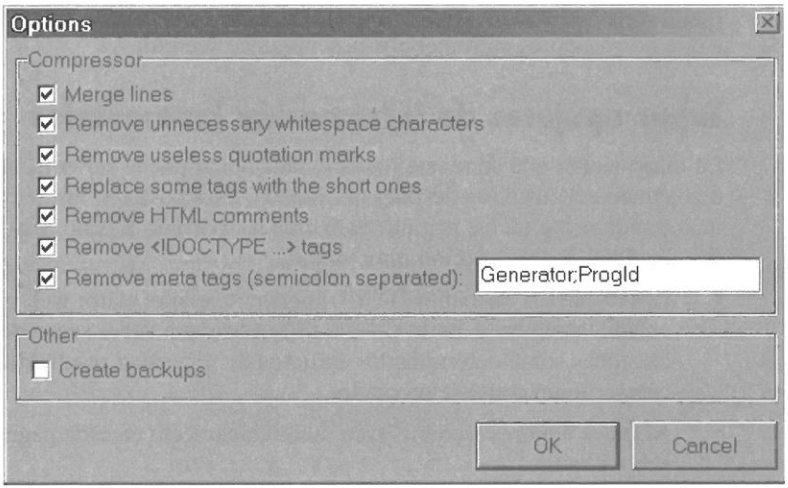
La información que se revela intencionadamente puede ser detectada mediante un examen exhaustivo y después, eliminada. Otra cosa son los datos publicados inadvertidamente en las páginas web creadas por uno mismo. Estos datos pueden ser tipos de información muy variada.

- Los meta-tags del editor HTML pueden revelar el editor web con el que fue creada la página. A partir de esta información, a veces se pueden sacar conclusiones sobre determinados agujeros de seguridad resultantes a raíz de la combinación con este producto.
- Algunos editores web incluyen automáticamente en cada página web datos sobre el autor.
- Aunque algunos comentarios no aparezcan en la propia página web, sí que están contenidos en el código fuente y pueden ser consultados.
- Los contenidos y las funcionalidades de versiones anteriores que no fueran borrados, sino sólo excluidos como comentarios, siguen estando en el código fuente y quizá puedan revelar información que en realidad ya no debería estar al alcance de todos.

Todas estas informaciones tienen algo en común: no tienen nada que ver con el contenido en sí de la página web, por lo que se puede prescindir de ellas. Esto permite recurrir a los llamados compresores HTML, que optimizan los archivos HTML. Eliminan todos los componentes que no sean importantes para el contenido de la página web y comprimen el archivo todo lo que pueden. Este proceso respeta el contenido verdadero y las páginas pueden seguir siendo visualizadas óptimamente por cualquier navegador web. Uno de estos compresores HTML es Absolute HTML Compressor, que podrá descargar gratuitamente como freeware en la dirección http://www.serpik.com.

1. Para depurar sus páginas web con el compresor HTML, arranque el programa y verifique, en primer lugar, si son correctas las configuraciones iniciales. Haga clic sobre *Options* de la barra de iconos para abrir las configuraciones.

2. Aquí, lo mejor es que active todas las opciones del área *Compressor*, para conseguir la máxima compresión. Con la casilla de opción *Create backups*, situada en la parte inferior, podrá decidir si antes de modificar los archivos HTML será necesario crear copias de seguridad. Si trabaja directamente con los archivos HTML originales, es recomendable que active esta opción. Guarde las configuraciones haciendo clic sobre el botón *OK*.



Configure las opciones del compresor HTML para una compresión máxima.

3. Active ahora la opción *Compress File* y haga clic sobre el botón *Browse...*, para indicar en un cuadro de selección de archivos el archivo que desee comprimir.

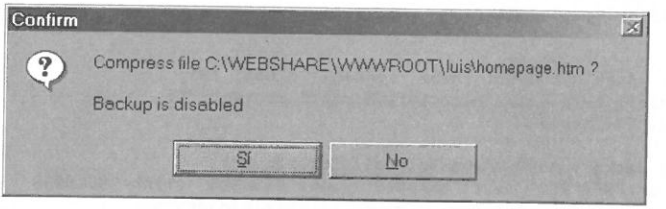
Indique qué archivo deberá ser comprimido.

TRUCO

Comprimir varios archivos

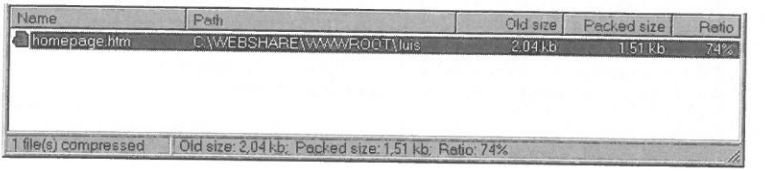
Absolute HTML Compressor también ofrece la posibilidad de comprimir simultáneamente varios archivos. Seleccione para ello la opción *Compress Files in a Folder* y seleccione el directorio con *Browse*. Si activa, además, la opción *Include subfolders*, también serán tenidos en cuenta los subdirectorios. Así puede comprimir de una sola vez todos los archivos de una página web.

4. Para arrancar el proceso de compresión, haga clic ahora sobre el símbolo *Compress*, situado en la parte superior izquierda de la barra de iconos. Confirme antes la consulta de seguridad con el botón Sí. Compruebe si la función de backup está activada o no. Si no lo está, las modificaciones que se hagan en el archivo HTML serán definitivas.



Confirme la consulta de seguridad anterior a la compresión.

5. Una vez concluida la compresión, verá en la parte inferior de la ventana principal una relación de los resultados. Aquí tienen especial interés las columnas *Old size* (tamaño anterior), *Packed size* (tamaño nuevo) y la proporción de reducción (*Ratio*). Son absolutamente normales las disminuciones en torno al 75%. En casos especiales, también podrían ser del 50% y más.

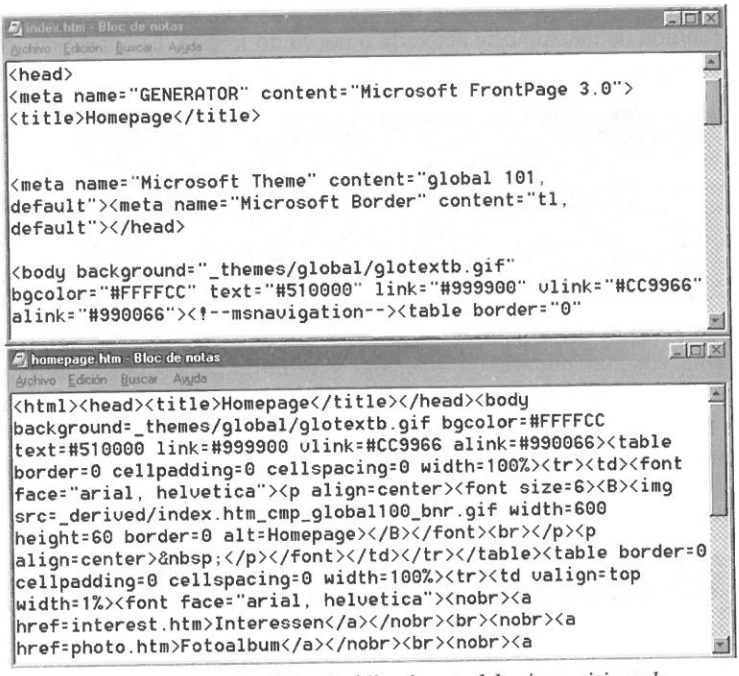


El archivo HTML fue comprimido al 74% de su tamaño original.

6. Acto seguido, podrá convencerse desde su navegador web que la página web sigue siendo representada como siempre.

Comprimir el código fuente

Si ahora observa el código fuente del nuevo archivo y lo compara con el del original, verá enormes diferencias. Por una parte, ahora faltan todos los elementos que no resultan necesarios para visualizar correctamente el contenido en el navegador web. Por otro lado, todo el archivo se ha vuelto mucho más compacto, por la sencilla razón de que el compresor ha encadenado directamente todos los elementos. Ya no queda rastro de ningún layout de líneas o de elementos similares, con los que en otras circunstancias trabajan editores humanos o de máquina. Eso hace que el código fuente sea extremadamente difícil de leer. Al navegador web esto no le molesta, pero a los fisgones entrometidos sí, ya que ahora no pueden extraer información del código, complicándoles la vida como se merecen.



Original y copia (comprimida): el código fuente del mismo sitio web.

Impedir el uso fraudulento de las imágenes publicadas

Otro peligro que surge al publicar páginas web es, que la información contenida en ellas podría ser aprovechada por otros para ponerle a usted en evidencia o en

ridículo. Con las imágenes contenidas en estas páginas, por ejemplo, podrían hacerse cosas muy extremas. Cualquiera que acceda a su página web personal, podría grabarse en su propio PC todos los gráficos que contengan y manipularlos después. Utilizando programas gráficos modernos, no hay que ser un profesional para crear con un poco de ingenio los fotomontajes más extravagantes; y si sólo le alargaran a usted la nariz o las orejas, podría darse por satisfecho. Pero no es nada infrecuente que las caras sean integradas en fotografías porno. Si una foto de esas llega a recorrer la empresa por e-mail, los demás tendrán más motivo de regocijo que usted.

El único modo de protegerse contra el uso ilícito de sus imágenes publicadas en páginas web, sería renunciar totalmente a ellas. Pero como eso sería una pena, intente publicar sólo imágenes de difícil manipulación.

- Las imágenes de baja definición no suelen ser demasiado vistosas, pero como los manipuladores de imágenes pensarán lo mismo, casi siempre las dejan en paz.
- Las imágenes en tonos de gris apenas permiten un coloreado posterior. Si son empleadas en fotomontajes, el resultado será de nuevo una imagen en tonos de gris. Este hecho también desalienta a muchos destructores de imágenes.
- Las imágenes muy comprimidas (por ejemplo JPGs con factores de compresión altos) son difíciles de manipular. Un aumento, una reducción o cualquier otro cambio reducen la calidad de imagen, por lo que casi siempre quedan inservibles.

9.2 Páginas web manipuladas

Aparte del peligro que supone que los contenidos de las páginas web sean usados para fines ilícitos, existe el riesgo de que las propias páginas web sean manipuladas. En este caso, los hackers se proporcionan acceso al servidor web y sustituyen los documentos web por páginas con contenidos propios. Este rediseño web se ha convertido en los últimos años en una nueva materia estándar para los hackers. Muchas veces, sólo lo hacen por diversión, para demostrar que son capaces de ello. Aunque para las víctimas, esto no supone ningún consuelo. Sin embargo, cada vez se dan más casos en los que se realiza un rediseño para causarle daños muy concretos al propietario de la página web. Por ejemplo, es fácil dañar la imagen de una empresa de la competencia, encargando a un hacker que filtre fotografías pornográficas en las páginas web de ésta.

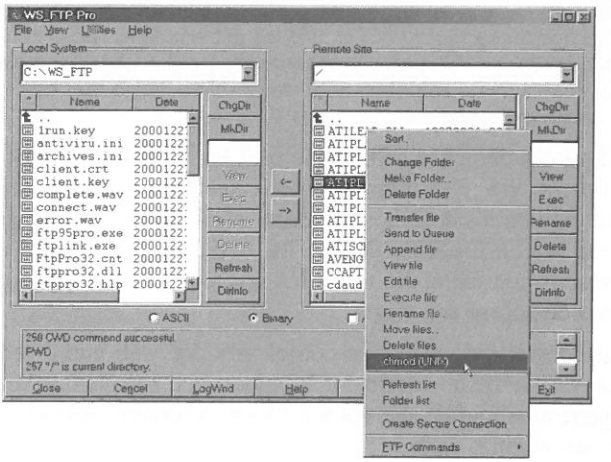
Con frecuencia, los hackers también atacan páginas web de instituciones conocidas, para llamar la atención de un gran número de visitantes y de los medios de comunicación sobre determinadas cuestiones. Organizaciones de renombre, como el FBI, la CIA, o importantes proveedores de Internet como Yahoo, ya

han sido víctimas de estos ataques. La agresión a UNICEF, presentada ya al comienzo de este capítulo, es uno de los ejemplos más notorios de ataques de rediseño perpetrados con éxito contra instituciones públicas.

Proteger las páginas web contra los ataques

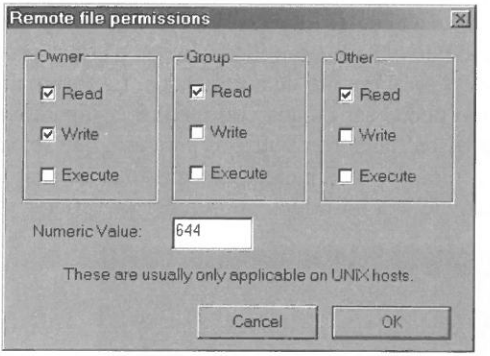
En principio, un ataque contra páginas web se puede realizar de dos formas diferentes. Por una parte, los hackers pueden atacar al propio servidor web. Al final de este capítulo, explicaremos cómo hacerlo. Una vez obtenido el acceso al servidor web, el hacker puede cambiar a su gusto los datos guardados en éste y con ello, también las páginas web. Aunque con frecuencia, ni siquiera hace falta esforzarse para penetrar en el servidor web, ya que a veces las propias páginas web están completamente desprotegidas por culpa de errores de configuración. Esto permite modificarlas y almacenarlas sin gran esfuerzo. Por lo tanto, es importante que cuando se coloquen archivos en el servidor web, se vigile la adjudicación de los derechos de acceso apropiados. Si usted lleva sus archivos al servidor web mediante FTP, debería almacenarlos ya con las correspondientes restricciones. Desgraciadamente, sólo pocos programas FTP ofrecen las funciones necesarias para esto. Un ejemplo positivo es *WS_FTP* Pro, del que encontrará una versión de prueba gratuita en la dirección http://www.ipswitch.com. Para todos los que obtengan regularmente archivos por FTP y, sobre todo, para los que quieran transmitirlos, WS_FTP es una herramienta excelente. La mayoría de sus funciones son equiparables a las de otros programas FTP y, además, vienen bien explicadas en el extenso archivo de ayuda. Aquí sólo pretendemos mostrarle lo que deberá tener en cuenta para asignar a sus archivos los derechos de acceso apropiados:

1. Traslade sus archivos como siempre al servidor web.
2. Marque con el mouse todos los archivos en el servidor remoto y, haciendo clic sobre ellos con el botón derecho del ratón, abra el menú contextual. Éste le facilitará algunas funciones, a las que de otro modo no podría acceder desde la interfaz de WS_FTP. Aquí encontrará, entre otros, el comando *chmod (UNIX)*.



Abra el menú contextual con el comando chmod.

3. Seleccione este comando. Con él abrirá el menú *Remote file permissions*, donde podrá configurar los derechos de acceso para los archivos en el servidor.



Ajuste los derechos de acceso para los archivos web.

INFO

Derechos de archivos bajo Unix

En los servidores Unix (y éstos son, con mucho, la mayoría de servidores web) hay tres clases de usuarios: *Owner* – usted como propietario de un archivo –, *Group* – un grupo de usuarios en igualdad de derechos, como por ejemplo todos los propietarios de una homepage en el servidor web – y *Other* – todos los demás usuarios de un ordenador servidor, que no entren en ninguna de las otras dos categorías –. En un servidor web esta categoría también incluye, entre otros, los visitantes que soliciten sus páginas web. Para cada categoría de usuarios, puede adjudicar individualmente los derechos de acceso. Conceda a todas las categorías de usuarios derechos de lectura

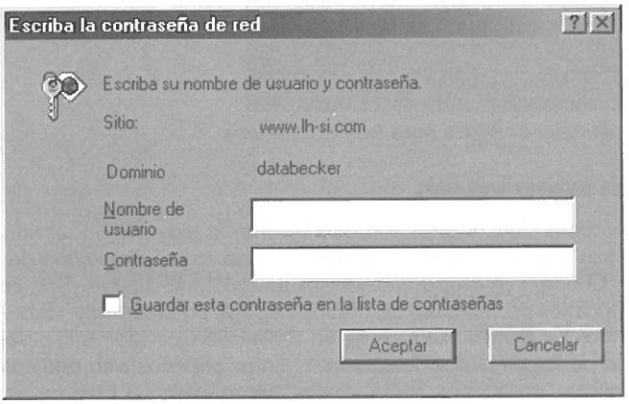
(*Read*), ya que de lo contrario nadie podría leer sus páginas. Sin embargo, los derechos de escritura (*Write*) sólo los debería tener usted como propietario de los archivos (*Owner*). Generalmente, los derechos para ejecutar programas (*Execute*) no son necesarios en absoluto, salvo que haya integrado algún script en la página.

4. Adjudique los derechos pertinentes para los archivos y confirme su selección con *OK*. WS_FTP transmitirá el comando correspondiente al servidor y éste cambiará los derechos de acceso según las instrucciones. Vigile que le llegue la confirmación de que los derechos de los archivos han sido modificados con éxito. No todos los servidores web soportan este tipo de derechos de acceso a archivos.

Si el método descrito no funciona con el servidor web que usted utilice, por ejemplo por tratarse de un ordenador Windows NT, sólo le quedará la posibilidad de dirigirse al administrador del servidor e informarse sobre los derechos de acceso para sus páginas web.

9.3 Contraseñas, archivos y áreas protegidas

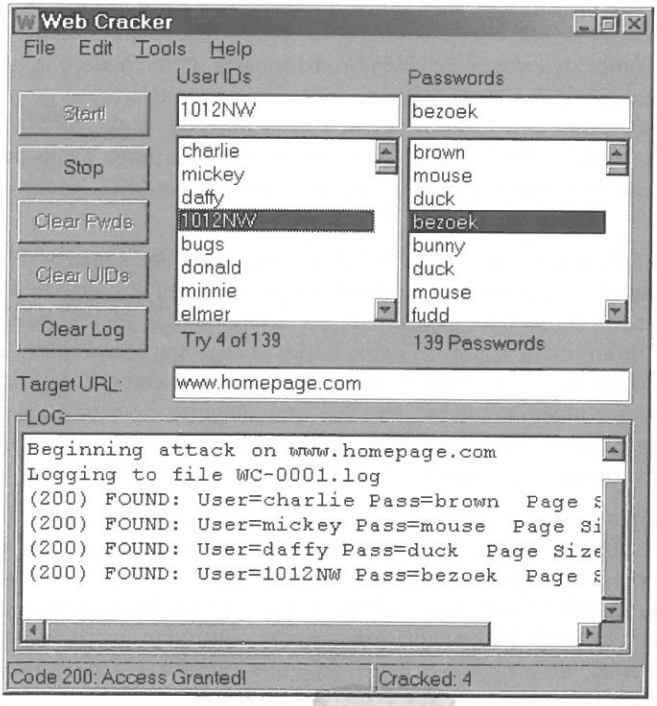
Se nos plantea un problema especial si no queremos que una parte de la página web esté al alcance de todos, sino que deseamos restringirla a un pequeño círculo de interesados, o quizá a clientes de pago. En este caso, hay que tener algún tipo de control de acceso que cuando sean llamadas las páginas protegidas verifique si el visitante pertenece al círculo de autorizados. La forma más simple de una consulta de este tipo puede ser creada con medios comparativamente fáciles. Los editores web ofrecen funciones sencillas para eso, que se ocupan de que cuando una página protegida sea solicitada, aparezca una ventana de contraseña de red, donde el visitante deberá introducir su nombre de usuario y contraseña.



Las páginas web para visitantes especiales pueden ser protegidas por una sencilla ventana de contraseña.

Desgraciadamente, estas funciones no son verdaderamente fiables. Los hackers han desarrollado programas que atacan selectivamente estas restricciones de acceso. Como las páginas pueden ser solicitadas a través de Internet, el ataque puede ser perpetrado desde cualquier lugar sin grandes problemas. Además, el número de intentos no suele estar limitado, por lo que un hacker podría efectuar con toda tranquilidad un ataque por fuerza bruta. Si encima, alguno de los usuarios eligió una contraseña insegura, el área protegida pronto dejará de estarlo.

Dentro de este manual no podemos presentar ningún método para hermetizar verdaderamente las páginas web, ya que esto es un tema aparte y nos saldríamos de nuestro propósito. Aquí sólo pretendemos hacerle ver que las soluciones sencillas casi siempre pueden ser burladas con facilidad. Si usted quiere proteger el acceso a su página web o a partes de la misma y si, además, ésta contiene datos confidenciales o críticos para su negocio, tómese la molestia de buscar una solución profesional; aunque quizá no le resulte precisamente barata. No obstante, si los datos son de verdad importantes y confidenciales, no debería escatimar gastos.



Con programas especiales, como Web Cracker, se pueden piratear por fuerza bruta las páginas web protegidas.

9.4 Posibilidades de ataque sobre servidores web

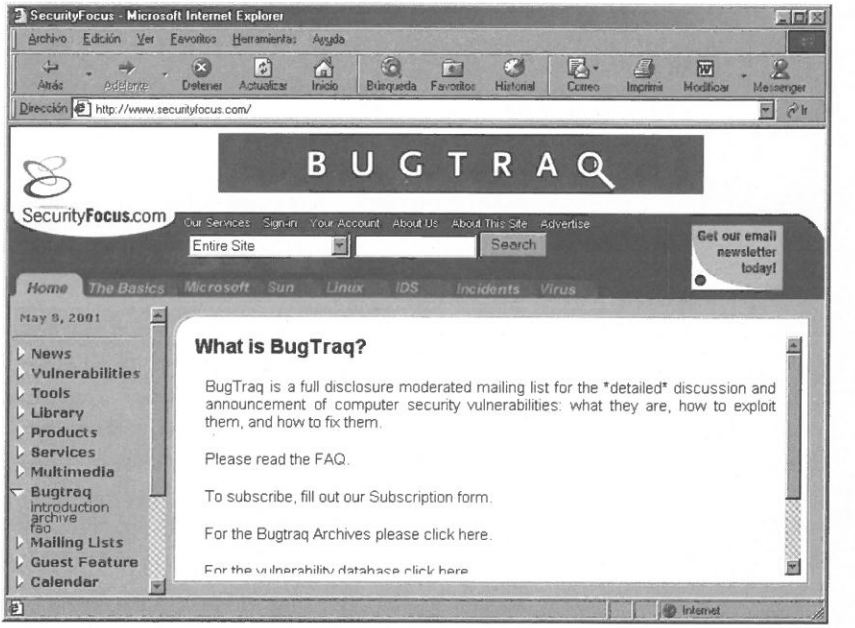
Aparte de los ataques a páginas web insuficientemente protegidas, a los hackers siempre les queda el recurso de atacar el propio servidor web. También aquí se distinguen dos tipos de posibles de ataques con los que se pueden sabotear páginas web.

- Un clásico ataque con irrupción, proporciona a los hackers acceso al servidor para hacerse con los derechos de administrador de ese ordenador. Una vez logrado el objetivo, el invasor podrá manipular a voluntad todos los datos almacenados en ese servidor; y como las páginas web, en definitiva, no son otra cosa que datos, podrán ser modificadas o borradas y sustituidas por otras páginas. En principio, un ataque de este tipo no se diferencia de cualquier otro ataque con irrupción, aunque persiga otros fines. El hacker dispone de todas las posibilidades. Después de todo, la mayoría de ataques de rediseño se basan en la irrupción en el ordenador servidor.
- Si lo que se pretende no es manipular una página web, sino simplemente inutilizarla, un servidor web ofrece posibilidades especiales. Como todos los productos de software complejos, los programas para servidores web no están exentos de errores. Se descubren sin parar deficiencias y agujeros de seguridad que quizá no faciliten la irrupción en el ordenador, pero sí pueden servir para inutilizarlo. A veces, estos puntos de ataque son alarmantemente sencillos. Por ejemplo, hubo servidores web cuya caída podía ser provocada simplemente con la introducción de una URL excesivamente larga.

En realidad, ambos tipos de ataque se basan en explotar los agujeros de seguridad (exceptuando la posibilidad de hacer social hacking, que brinda el ataque con irrupción). El problema especial para los operadores de páginas web es, que sólo pueden influir en la seguridad del servidor si explotan un servidor web propio. Pero si, como ocurre en muchos casos, sólo se alojan como huéspedes en un servidor web que alberga, además, muchas otras páginas, apenas se puede controlar el trabajo del servidor. Aquí sólo queda la posibilidad de confiar en la cualificación del administrador del servidor.

Es importante que se mantenga al día constantemente. Emplee siempre la versión más actualizada de su software de servidor. Aparte de esto, esté al corriente de los problemas recién detectados y de los agujeros de seguridad e instale lo antes posible los parches adecuados. http://www.upenn.edu/computing/security-privacy es una magnífica dirección donde podrá conseguir en todo momento, a través de Internet, información actualizada sobre este tema. Son especialmente interesantes en esta página los subdirectorios */standards*, donde encontrará estándares de seguridad para sistemas operativos; */standards/wwwsec.html*, que hace especial hincapié en los servidores web; así como */SecurityPatches.html*,

donde hay una relación de los parches relevantes para la seguridad ofrecidos por renombrados proveedores de productos. En este contexto, también tiene interés la *WWW Security FAQ* bajo la dirección www.w3.org/Security/Faq/www-security-faq.html. Para conocer enseguida los errores de software y los agujeros de seguridad recién descubiertos, resultan indicadas las listas de correo. Usted puede abonarse a algunas especializadas en este tema, como por ejemplo la lista *Bugtraq*, en la dirección *http://geek-girl.com/bugtraq/*.



Bajo www.securityfocus.com, se puede abonar a varias listas de correo relacionadas con temas importantes para la seguridad.

10. ¿Alternativas seguras? – Linux, Windows NT/2000 y Co.

10.1 El hermano mayor: Windows NT/2000 519
Windows NT/2000 contra Windows 9x/ME 520
El administrador de usuarios en Windows NT/2000 522
10.2 Barato, ¿pero también seguro? – Linux como alternativa 523
Linux: Unix económico para PCs 524
Hacer segura la instalación de Linux 528

En los capítulos anteriores ha quedado patente que todos los sistemas operativos Windows en sus versiones 9x/ME presentan algunas debilidades, resultantes del principio básico del propio sistema. En algunos casos, éstas sólo pueden ser eliminadas con un esfuerzo considerable por parte del usuario y mediante el concurso de programas adicionales, mientras que en otros ni siquiera pueden ser corregidas. Eso hace que nos preguntemos si no existen alternativas a estos sistemas que sean igual de prácticas, pero más seguras. En este capítulo, queremos ir al fondo de la cuestión, profundizando sobre todo en los sistemas Windows NT/2000 y Linux.

10.1 El hermano mayor: Windows NT/2000

Windows 9x/ME ha sido diseñado por su fabricante Microsoft como lo que ellos denominan un sistema operativo SoHo, lo que viene a significar *Small-Office/Home-Office*; esto es, está enfocado a pequeñas empresas o al ámbito casero. No obstante, Microsoft también ofrece un producto para uso profesional. Hasta hace poco, este producto se llamaba Windows NT, tratándose de un sistema que sigue estando ampliamente difundido hoy en día. Pero la versión más reciente atiende al nombre de Windows 2000. En lo sucesivo, emplearemos indistintamente ambos conceptos, ya que para nuestras reflexiones las diferencias entre Windows NT y el reciente Windows 2000 son insignificantes. Este último, no deja de ser un perfeccionamiento de su predecesor, aunque a Microsoft le guste venderlo como un producto totalmente nuevo.

Windows NT y la seguridad

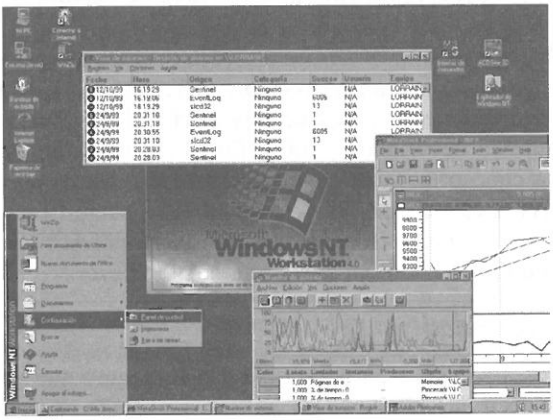
La primera reflexión es, sin duda, si Windows NT es más seguro que su hermano pequeño. Se puede decir que Windows NT ha sido concebido como un sistema operativo profesional que puede ser empleado en entornos críticos para la

empresa. Como tal, dispone realmente de un concepto de seguridad bastante más sofisticado que las versiones 9x/ME. Así, Windows NT tiene un administrador de usuarios que realmente merece este apelativo. Para cada usuario se pueden generar directrices, que regulan con exactitud lo que puede hacer y lo que no. Estas directrices son controladas por el sistema y, en contraste con Windows 9x/ME, Windows NT ha sido concebido para que vigile rigurosamente el cumplimiento de las reglas y no permita infracciones. A las configuraciones y funciones críticas sólo pueden acceder aquellos usuarios que antes hayan sido definidos expresamente como administradores y dispongan de los derechos pertinentes. Esto hace que un sistema Windows NT esté mucho mejor protegido contra manipulaciones no permitidas.

Como, además, Windows NT va destinado desde un principio a ser usado en entornos de red, facilita funciones de red mucho más extensas, a la vez que está provisto de mejores medidas de seguridad. El problema es que estas funciones, si bien amplias, también complican mucho la configuración de un sistema Windows NT, con lo que se incrementa el peligro de hacerlo mal, lo que a su vez puede derivar en importantes agujeros de seguridad.

Windows NT/2000 contra Windows 9x/ME

Naturalmente, todo lo expuesto plantea la cuestión de dónde están las diferencias entre las dos familias Windows y si realmente es tan sencillo cambiar de Windows 9x/ME a Windows NT/2000. En principio, la superficie presenta grandes similitudes entre las dos familias de sistemas operativos. No en vano, ambas proceden de la misma casa: Microsoft. La interfaz y su manejo fundamental son muy similares. Sólo hay diferencias en el ámbito de configuración y de la herramienta de administración, cosa que por otra parte es inevitable si se pretende que un sistema sea mejor que el otro.



El entorno gráfico de Windows NT y los de Windows 9x/SE ME se parecen como dos gotas de agua.

Software para Windows NT

De un modo u otro, como usuario de Windows no hay que preocuparse por la cuestión de conseguir aplicaciones. Ambos sistemas son binariamente compatibles, hasta el punto de que los programas de Windows pueden ejecutarse tanto bajo Windows NT como bajo Windows 9x/ME, sin que se requieran versiones diferentes. Por lo tanto, quien cambie de un sistema a otro, generalmente, podrá seguir usando todos los programas ya existentes, aunque podrían producirse problemas en algunas áreas, por ejemplo las que exijan capacidades multimedia especiales. En este aspecto, Windows NT no está tan desarrollado como Windows 9x/ME. A fin de cuentas NT está destinado a usos profesionales, no a jueguecitos y diversión. Sobre todo la cuestión de los juegos es un tema más bien sombrío.

Juegos, ¡no, gracias!

Los juegos de ordenador y Windows NT son un tema espinoso. Muchos juegos sofisticados que se ejecuten, por ejemplo, con elementos 3D no funcionarán con Windows NT. Quien tenga afición a los juegos y los utilice mucho debería conservar también Windows 9x/ME. A fin de cuentas, los juegos suelen ser desarrollados para los sistemas predominantes en el ámbito privado, es decir, Windows 9x/ME. Una ayuda la podría prestar la tecnología DirectX, ofrecida por Microsoft para los dos sistemas. Según este nuevo estándar, los juegos basados en DirectX también deberían funcionar en ordenadores con Windows NT, aunque en la práctica, esto dista mucho de ser siempre así. Aunque el nuevo Windows 2000 vaya por buen camino, también aquí surgen constantemente problemas, pero se supone que en el futuro, sobre todo los juegos en 3D que necesiten mucha potencia, podrán funcionar más deprisa y mejor bajo Windows 9x/ME.

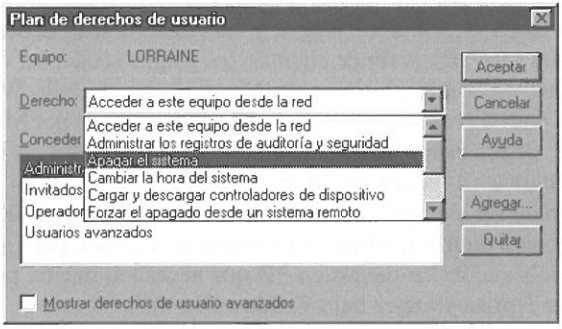
Hardware para Windows NT

Bajo Windows NT, el hardware se puede convertir en un problema. Windows NT emplea un modelo de driver diferente a Windows 9x/ME, y Windows 2000, a su vez, otro modelo distinto. Esto hace que los drivers de hardware para Windows 9x/ME sólo puedan ser empleados en muy pocos casos bajo Windows NT o Windows 2000. En lugar de eso, se requieren drivers especiales que muchos fabricantes de hardware ni siquiera ofrecen. En los componentes estándar, como adaptadores RDSI y tarjetas de sonido, muchas veces se tiene suerte y se encuentra un driver. En algunos casos, Microsoft también pone a disposición drivers genéricos que trabajan con muchos componentes. Pero un hardware más exótico podría convertirse en un verdadero problema. Aquí convendría consultar sin falta al fabricante y averiguar si su hardware está soportado bajo Windows NT.

El administrador de usuarios en Windows NT/2000

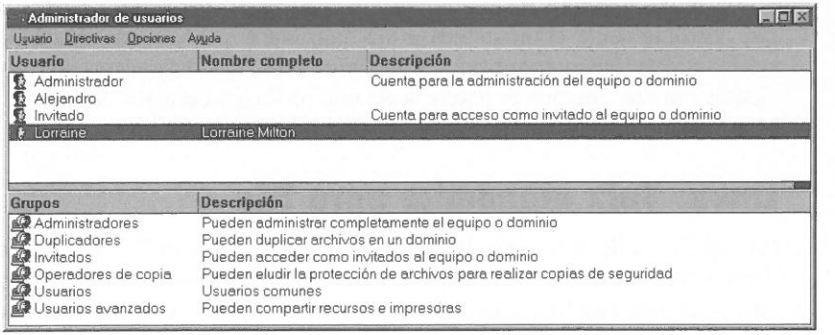
Una de las diferencias fundamentales entre Windows NT/2000 y Windows 9x/ME es el administrador de usuarios. Según lo expuesto en el Capítulo 2, también el Windows "pequeño" dispone de un administrador de usuarios. Aunque ya hemos puntualizado que este no protege realmente los datos y las funciones importantes y confidenciales, sino que sólo los oculta, por lo que incluso poseyendo conocimientos rudimentarios se pueden ver todos los datos y usar todas las funciones. Sólo programas adicionales como *eSafe* permiten instalar una protección realmente eficaz que merezca el calificativo de administrador de usuarios.

En este aspecto, Windows NT es diferente, ya que aporta de origen un administrador de usuarios competente. En principio, su funcionamiento es similar al otro, es decir, cada usuario del ordenador recibe un nombre de usuario y una contraseña que le servirán para hacer login en el sistema. Con esto, el sistema operativo sabrá qué derechos corresponden a ese usuario y a qué recursos puede acceder.



Para cada usuario se pueden establecer directrices concisas sobre las funciones que pueda ejecutar.

Para hacer más sencilla la administración de muchos usuarios en un sistema, Windows NT añade el concepto de grupos de usuarios. Un grupo es algo así como un usuario virtual, para el que han sido definidos determinados derechos de acceso. El grupo *Administradores*, por ejemplo, posee todos los derechos de acceso y tiene permiso para cambiar la configuración completa del sistema. Los *invitados*, por el contrario, sólo son usuarios temporales y apenas les corresponden derechos de acceso. Al dar de alta un nuevo usuario, se le puede asignar a dicho usuario uno de esos grupos o varios. Así, este usuario recibe automáticamente todos los derechos de acceso del grupo al que pertenezca. Por lo tanto, si un nuevo usuario es asignado al grupo de administradores, recibirá automáticamente todos los derechos de acceso sin necesidad de liberar expresamente cada uno de los derechos. Este concepto por grupos facilita enormemente la administración de los usuarios.



En Windows NT los usuarios pueden ser clasificados en grupos, con lo que es más fácil administrarlos.

10.2 Barato, ¿pero también seguro? – Linux como alternativa

Quien quiera alejarse definitivamente de la escudería Windows de Microsoft encontrará en la gama Unix una atractiva alternativa. Unix es un sistema operativo diseñado desde el principio para trabajar en entornos de red. Por consiguiente, dispone de un concepto de seguridad diferenciado, basado en el planteamiento de que todos los datos y recursos pertenecen a un usuario. Sólo ese usuario tiene acceso ilimitado. Si también quiere acceder otro, se le deberán asignar expresamente los correspondientes derechos. El propio sistema vigila que los derechos de acceso sean respetados. Esto hace prácticamente imposible la existencia de abusos accidentales o intencionados, aunque no significa que los sistemas Unix sean automáticamente herméticos. Precisamente por sus múltiples funciones de red entrañan también riesgos. Por una parte se descubren constantemente agujeros de seguridad y, por el otro, la configuración de un sistema Unix es muy difícil. Esto hace que precisamente los usuarios inexpertos cometan pequeños errores, que con el tiempo pueden llegar a redundar en graves consecuencias para el sistema. A pesar de todo, un ordenador Unix bien configurado es una alternativa real a un PC con Windows.

Y ahora, ¿cómo trasladar Unix al PC de casa? Los "verdaderos" sistemas Unix como AIX o Solaris no se dejan instalar en un PC normal, ya que trabajan sobre arquitecturas especiales de hardware y, por lo general, también en cuestión de memoria son bastante más generosos que un PC de uso corriente. Con arreglo a eso desarrollan un potencial de rendimiento mayor. Aunque también hay algunos derivados de Unix especiales (variantes), que han sido desarrollados especialmente para el PC; se trata de versiones que adaptan el modo de funcionamiento básico de Unix a los procesadores x86 habituales en un PC normal.

Los sistemas gestados de este modo son "pequeñas" versiones de Unix completas, absolutamente comparables a sus hermanos y hermanas mayores por el modo de funcionamiento básico y sus interfaces. Las diferencias sólo son apreciables bajo la carcasa: la potencia de una moderna estación de trabajo de Sun es imposible de alcanzar por muy bien equipado que esté un PC.

Linux: Unix económico para PCs

Hay una serie de derivados de Unix que son aptos para el PC, aunque el que va claramente en cabeza es el sistema Linux, ya que a nivel mundial es, con diferencia, el más difundido. Lo más destacable de Linux es el hecho de que no se trate de un producto comercial (hace algunos años, ninguna empresa de software habría pensado seriamente que se pudiera ganar dinero con un Unix para PCs). Linux se remonta a la idea original de su "inventor", Linus Torvalds, que un buen día se hartó del sistema operativo DOS y quiso trabajar en su PC igual que en un ordenador Unix, por lo que empezó a desarrollar su propio sistema operativo, que debía ser capaz de trabajar exactamente igual que Unix. Con el tiempo fue encontrándose cada vez con más gente a la que le entusiasmaba la idea y que aportó su parte al software. De este modo, se germinó un sistema operativo que con los años se fue perfeccionado cada vez más y maduró. Si al principio sólo lo podían sacar adelante los verdaderos expertos y los "freaks", ahora ya hay distribuciones cómodas que no tienen nada que envidiar a un equipo Windows.

INFO

¿Es Linux realmente gratuito?

Como característica especial de Linux siempre se resalta su gratuidad. De hecho , no es un producto comercial, es decir, ninguna de las personas implicadas en su desarrollo gana dinero con él. Los archivos necesarios para una instalación de Linux, por ejemplo, pueden ser descargados íntegramente de Internet. Pero esta instalación supone un gran esfuerzo y resulta muy laboriosa, por lo que sobre todo los usuarios noveles difícilmente pueden llevarla a cabo. Por ello, existe lo que se denomina como distribuciones Linux o "distros". Estas distribuciones son colecciones de todos los archivos necesarios y que pueden ser obtenidos, por ejemplo, en CD-ROM. Las empresas que ofrecen estas distribuciones recopilan esos archivos y los equipan con una rutina de instalación más o menos cómoda para que hasta los principiantes absolutos puedan instalar y configurar sin problemas su nuevo sistema Linux. Aunque estas distribuciones no son gratuitas; a fin de cuentas, es natural que las empresas quieran obtener un beneficio por su esfuerzo, ni con mucho resultan comparables sus precios con los de una nueva versión de Windows. En algunos casos, ya se pueden adquirir distribuciones Linux a precios módicos, por ejemplo como suplemento de una revista de informática. La selección de distribuciones, además, es muy grande. La de mayor difusión a escala mundial es *Red Hat*, mientras que en Europa (especialmente en los países de habla alemana) SuSE es la que lleva la delantera, al ofrecer esta empresa

una versión de Linux muy completa y en su mayor parte traducida a una gran variedad de idiomas. Por cierto, una vez instalado Linux por distribución, todas las demás ampliaciones y actualizaciones podrán ser descargadas de Internet de forma completamente gratuita. Sólo si las innovaciones son importantes merece la pena comprarlas para ahorrar tiempo y costes de descarga.

Linux contra Windows

Pero, ¿resulta Linux equiparable a Windows? Algunos prejuicios afirman que el manejo de Linux es mucho más complicado. Otros hacen referencia a la falta de software y a los problemas que surgen cuando se emplea hardware adicional. Nosotros vamos a intentar enfocar objetivamente los puntos decisivos.

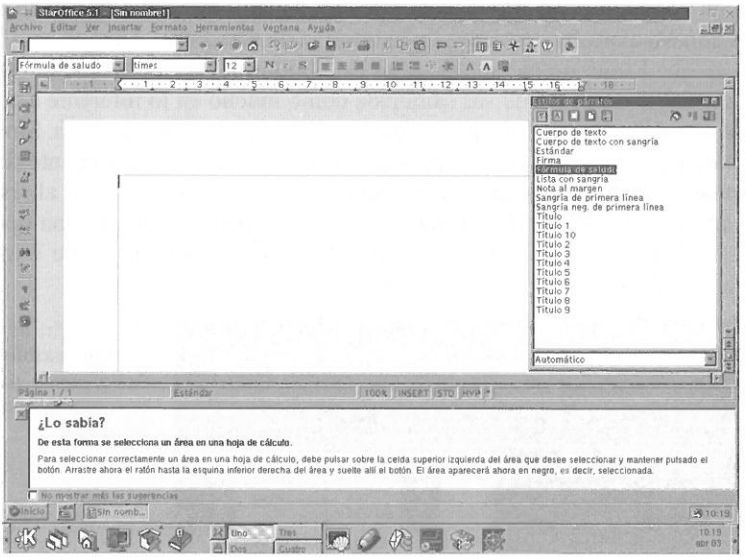
Comodidad en el manejo

El manejo siempre es cuestión de gustos. El usuario fiel de Windows tendrá arraigados unos hábitos con lo que, al principio, cualquier otro concepto le parecerá en conjunto peor. ¡Pero pregunte a un usuario que haya trabajado muchos años con Macintosh qué piensa de la interfaz de Windows! Aunque aquí lo decisivo es que Linux no es tan diferente de Windows. Éste tiene una interfaz fija, cuya configuración puede ser cambiada como mucho en lo referente a colores y al fondo del escritorio, sin cambiar para nada la funcionalidad básica. Sin embargo, para Linux hay varias interfaces que, además, son extremadamente flexibles. Algunas distribuciones aportan, también, entornos adicionales al estilo de Windows, para facilitar la adaptación a los usuarios de este sistema operativo. De este modo, la interfaz de Linux tiene el mismo aspecto que la de Windows y se deja manejar casi del mismo modo.

La interfaz de Linux es muy flexible y, si se desea, puede asemejarse mucho a la de Windows.

Software disponible

Con Linux no se pueden seguir empleando sin más las aplicaciones a las que se esté habituado con Windows. Hay muy pocos programas disponibles conjuntamente para ambos sistemas. Sobre todo, muchas aplicaciones estándar, como por ejemplo las de Microsoft (Word, Excel, Access, etc.), no están disponibles para Linux. Aunque también en estos casos existen alternativas útiles. StarOffice, por ejemplo, puede adquirirse también en una versión para Linux, e incluso descargarlo completamente gratis. El paquete KOffice fue especialmente diseñado para el entorno KDE de Linux y, en la actualidad, el alcance de sus funciones no tiene nada que envidiar al de otras aplicaciones. Por lo tanto, los usuarios particulares pueden estar seguros de que también para Linux encontrarán los programas apropiados, aunque a veces sean algo diferentes. A cambio, el software para el sistema operativo gratuito de Linux, en la mayoría de los casos, también es gratis – ¡Si esto no es un buen argumento... ! – Aún con todo, antes de cambiar a Linux, el usuario de PC profesional debería informarse detalladamente sobre los programas disponibles para su actividad y si éstos son realmente útiles.



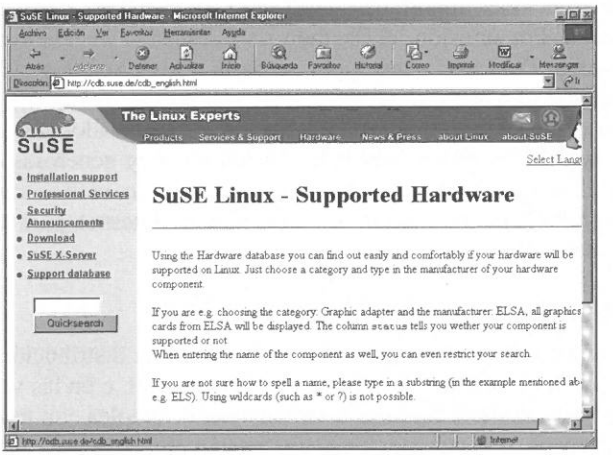
El procesador de texto de StarOffice para Linux es un magnífico sustituto de Microsoft Word.

Hardware disponible

Sin duda, la disponibilidad de hardware sigue siendo uno de los talones de Aquiles de Linux. Naturalmente, en principio se puede incorporar a un PC bajo Linux cualquier hardware, igual que a un PC bajo Windows. Después de todo,

el PC es el mismo. El problema son los drivers necesarios para que funcione el hardware, que prácticamente establecen el contacto entre el hardware y el sistema operativo. Hoy en día, se puede encontrar un driver para Windows en cualquier tarjeta gráfica, escáner y adaptador RDSI. Los drivers de Linux, sin embargo, siguen siendo la excepción absoluta. Aunque esto no quiere decir que Linux no sirva para nada. Las tarjetas gráficas, por ejemplo, no suelen causar ningún problema. También los módems externos para la conexión a Internet pueden ser utilizados sin inconvenientes por su modo de funcionamiento. Las tarjetas RDSI ya plantean más dificultades. Para los modelos estándar de gran difusión suele haber casi siempre una solución, pero a los exóticos a veces resulta imposible hacerles funcionar. El problema es que muchos fabricantes de hardware ven su clientela exclusivamente en la comunidad Windows, por lo que aplican toda su energía y sus recursos al desarrollo de drivers para Windows. Pero como las interioridades de Linux son completamente diferentes a las de Windows, no se puede sacar ningún provecho de estos drivers, por lo que la comunidad Linux debe desarrollar sus propios drivers para cada nuevo hardware. Como esto es una actividad que se suele realizar voluntariamente y en el tiempo libre, por supuesto lleva algún tiempo. Así que para los aparatos muy exclusivos, seguramente habrá quien nunca llegue a tener un driver.

Quien se atenga al hardware estándar, no tendrá muchos problemas con Linux. Pero si usted incorpora componentes de hardware diferentes, como por ejemplo tarjetas de captura de vídeo o adaptadores de red especiales, sería recomendable que consulte antes si pueden funcionar bajo Linux. En la Red es posible encontrar información al respecto, concretamente en http://www.suse.com, donde podrá consultar una base de datos de soporte de hardware, siempre que sepa el fabricante y el modelo del producto en cuestión.



Bajo http://www.suse.com encontrará usted la base de datos de hardware de la distribución SuSE-Linux.

Hacer segura la instalación de Linux

Desde luego, hay algo que tampoco se puede decir de Linux: que sea fundamentalmente más seguro que Windows. Linux aplica el concepto de seguridad, es decir, también aquí cada archivo y cada proceso tiene un usuario y sólo se permite el acceso a quien disponga de la autorización pertinente. En este sentido, Linux es claramente superior a los sistemas de Windows. Aunque por otro lado, comparte con Unix las múltiples funciones de red. Éstas pueden acabar siendo auténticas debilidades, ya que la mayoría de las distribuciones Linux instalan y activan de forma estándar un sinfín de servicios de red aunque el usuario no los necesite en absoluto. Pero estos servicios de red innecesarios pueden originar, a veces, peligrosos agujeros de seguridad cuando el usuario se conecte a Internet con su PC Linux, ya que entonces esos servicios, con todos sus agujeros de seguridad y sus configuraciones incorrectas, quedan expuestos a los atacantes de todo Internet. Por ello, para concluir este capítulo queremos mostrarle cómo hacer que su PC Linux sea seguro. Nos vamos a orientar por la distribución SuSE, ampliamente difundida en Europa. Las otras distribuciones pueden emplear, a veces, interfaces de configuración distintas, de modo que el proceso podrá diferenciarse en algunos detalles, pero no en el principio fundamental. Por eso, como complemento, vamos a exponer también un método general que puede ser aplicado en todas las instalaciones Linux.

El daemon de Internet y sus servicios

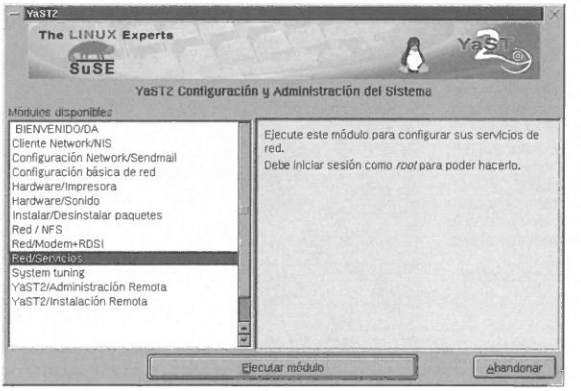
En Linux, todos los servicios de Internet son controlados por un componente central llamado daemon o demonio de Internet, abreviado *inetd*. Se denomina como daemon a todo proceso central que se ejecute permanentemente en segundo plano y facilite funciones importantes. Podríamos calificarles de espíritus serviciales del sistema. Por omisión, el daemon de Internet se instala durante el arranque del sistema. Después, arranca por su parte a los propios servicios de Internet, como el servidor web, el servidor FTP y el acceso Telnet. El usuario puede configurar con exactitud qué servicios deben ser arrancados. En la instalación estándar, las distribuciones habituales suelen ser muy generosas e instalan todos los servicios que pueda necesitar el usuario. Por eso, le recomendamos que verifique sin falta la configuración de su daemon de Internet, para adaptarla a sus necesidades reales.

Configurar los servicios de Internet mediante Yast

La forma más cómoda de hacer estas configuraciones en la distribución SuSE, por ejemplo, es utilizar la herramienta de configuración *Yast*, o en las versiones más recientes el *Yast2* gráfico. En otras distribuciones se emplea con frecuencia el programa *linuxconf*, que aunque tenga un aspecto algo diferente, ofrece la misma funcionalidad básica.

1. Para ajustar los servicios de red de su PC bajo Linux, arranque Yast o Yast2. Esto se hace a través del menú de inicio del escritorio, o introduciendo el comando correspondiente en una pantalla de terminal. Por favor, tenga en cuenta que para hacerlo deberá estar dado de alta como root o administrador. Yast funciona en cualquier entorno, mientras que para la interfaz gráfica de Yast2 necesitará un servidor X en marcha.

2. En el menú de inicio de Yast2, usted puede elegir entre varios módulos. Haga clic aquí sobre la opción *Red/Servicios* y después sobre el botón *Ejecutar módulo*, situado en el margen inferior de la ventana.



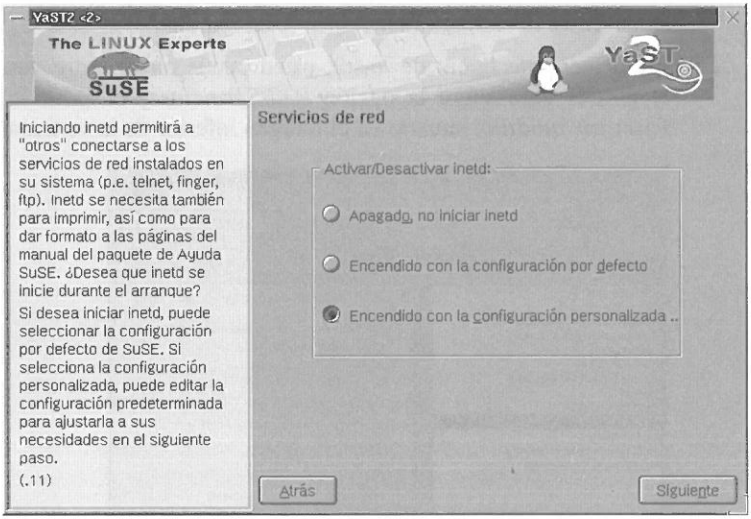
Seleccione en el menú principal de Yast el módulo Red/Servicios.

3. Con esto se inicia el módulo de los servicios de red, donde podrá definir, en primer lugar, el comportamiento básico del daemon Inet.

4. Si usted quiere renunciar totalmente a los servicios de Internet, puede desactivar del todo el daemon de Internet. Seleccione para eso la opción *Apagado, no iniciar inetd*. El daemon inetd ni siquiera será activado durante el arranque del sistema, por lo que no podrá arrancar ningún servicio de Internet. Esta opción es la más segura si usted no quiere tener nada que ver con Internet. Por otro lado, podría afectar también a servicios internos que quizá no funcionen sin daemon inetd. Por ejemplo, podría haber problemas a la hora de imprimir. Además, el sistema de ayuda interno ya no funcionará óptimamente, por depender del servidor web que es iniciado por daemon inetd.

5. Con la opción *Encendido con la configuración por defecto*, se activa el daemon inetd con la configuración que fue implantada durante la instalación de Linux, es decir, con las especificaciones del distribuidor. Este ajuste puede ser conveniente, ya que así queda garantizado el funcionamiento de todos los servicios necesarios, como por ejemplo los sistemas de ayuda. Aunque de este modo, usted volverá a abrir todos los agujeros de seguridad.

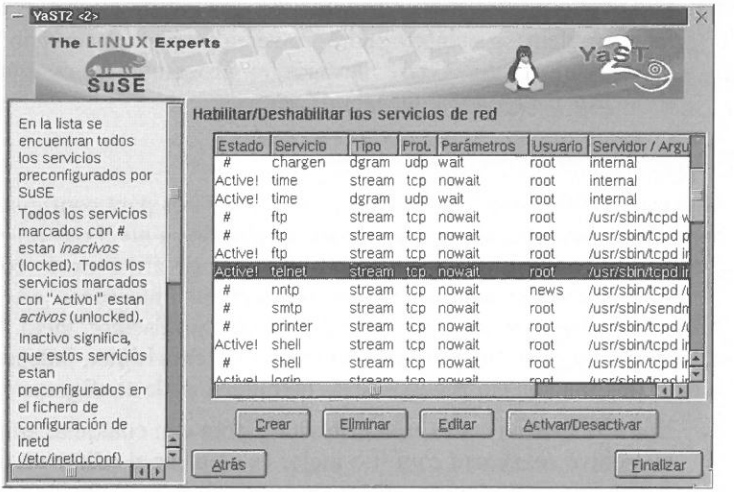
6. Lo mejor es que defina su propia configuración para daemon de Internet, mediante la opción *Encendido con la configuración personalizada*. En un paso posterior, podrá establecer con exactitud qué servicios de Internet deberán funcionar y cuáles no.



Elija en primer lugar si hay que arrancar el daemon de Internet y cómo deberá hacerse.

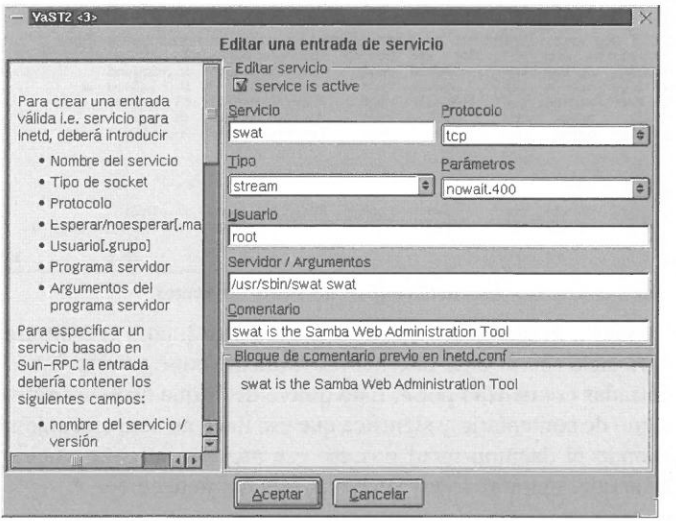
7. Si ha elegido la versión personalizada, recibirá en el siguiente paso un cuadro de conjunto de la configuración que tiene en ese momento daemon de Internet. En ella figuran todos los servicios que daemon inetd puede arrancar en principio. En la entrada *Estado*, se puede ver qué servicios funcionan con la configuración actual. Podrá reconocerlos fácilmente por llevar el estado *Active!*. Por el contrario, los servicios que lleven el estado # no serán activados.

8. Para cambiar el estado de un servicio, seleccione la entrada correspondiente en la lista y haga clic sobre el botón *Activar/Desactivar*. Con esto debería cambiar inmediatamente la entrada del estado. Aunque el servicio no será desactivado realmente, hasta que no cierre el programa de configuración.



La configuración definida por el usuario le permite desactivar individualmente los diferentes servicios.

9. Lo mejor será que repase toda la lista y compruebe, para cada servicio activo, si lo necesita realmente. Con *Editar*, usted puede llamar para cada servicio un menú, donde en la categoría *Comentario* encontrará una breve descripción del mismo.



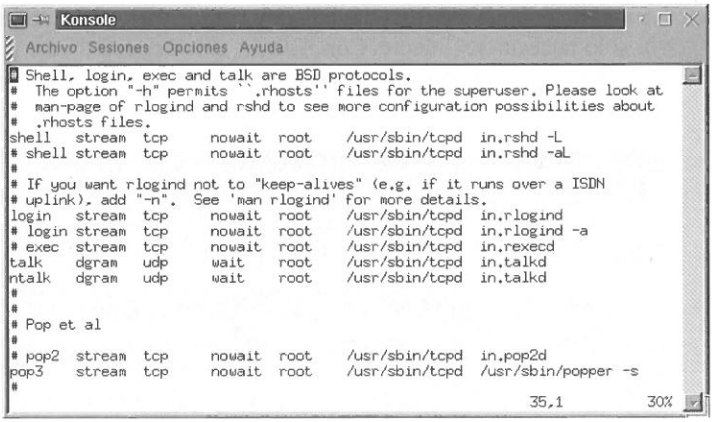
Por lo general, en el menú de procesamiento encontrará referencias a la función de un servicio.

10. Siempre es preferible que desactive de más que de menos. Si esto le originara problemas, siempre podrá volver a activar el servicio en cuestión según lo descrito. Cierre después el programa de configuración con *Finalizar* para guardar las modificaciones.

Cambiar directamente inetd.conf

Mientras en Windows prácticamente todos los datos para configurar el sistema operativo y las aplicaciones pueden ser localizados a nivel central en la base de datos del registro, Linux trabaja con un sinfín de archivos de configuración. También existe uno para el daemon de Internet. Procesando este archivo, se puede modificar directamente la configuración del daemon inetd. Este método ofrece la ventaja de que trabaja en cualquier sistema Linux, independientemente de la distribución empleada y de las herramientas de configuración existentes.

1. Entre al sistema como administrador y abra con cualquier editor de textos el archivo */etc/inetd.conf*. Lo mejor es emplear el editor *vi*, que funciona con textos en cualquier ventana de terminal. Pero también puede recurrir a un cómodo editor que funciona bajo la interfaz gráfica.

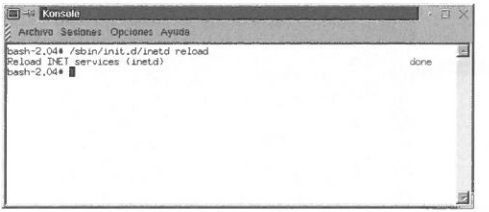


Abra el archivo /etc/inetd.conf en un editor de textos.

2. Similar a lo que hemos explicado para Yast2, aquí encontrará una entrada para cada servicio de Internet previamente configurado. La mayoría de las entradas comienzan por #. Esto quiere decir que no están activadas. # es un signo de comentario y significa que esa línea no será ejecutada. Por lo tanto, cuando el daemon inetd procese ese archivo de configuración durante el arranque, ignorará todas las líneas que comiencen con #.

3. Esto implica que un servicio activo pueda ser desactivado con suma sencillez, con sólo añadir al comienzo de la línea correspondiente el signo de comentario #.

4. Cuando usted haya hecho las correspondientes adaptaciones en el archivo inetd.conf, guárdelo y cierre el editor. En *vi*, esto puede hacerse con *[Esc]*, *[:]* y *[w]* (*w* significa *write*, en español "Escribir") y *[Esc]*, *[:]* y *[q]* (*q* significa *quit*, en español "Finalizar").
5. Cambie ahora a una de las consolas de entrada de datos (si no empleaba ya una para el vi). ¡Tenga en cuenta que también para el siguiente paso deberá estar obligatoriamente dado de alta como usuario *root* o administrador!
6. El archivo de configuración sólo es procesado durante el arranque del daemon de Internet, es decir, sólo cuando arranca el sistema. Pero para activar los cambios, no es necesario que usted apague todo el sistema Linux y lo vuelva a iniciar. Basta con que haga al daemon inetd en funcionamiento una señal, para que él mismo se reinicie. Esto hará que el archivo de configuración sea procesado de nuevo y entren en vigor las modificaciones. Introduzca para ello el comando */sbin/init.d/inetd reload*.



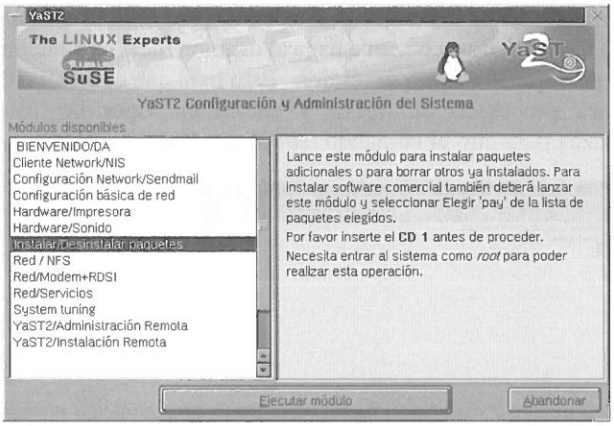
Vuelva a arrancar el daemon inetd, para que la configuración nueva sea activada.

Con esto, usted ha reiniciado el daemon de Internet con la nueva configuración y todo el proceso no le habrá llevado más de uno o dos segundos. Para realizar esta tarea bajo Windows, habría hecho falta un rearranque completo. Digo esto sólo como pequeño comentario a añadir a la comparación entre Windows y Linux.

Desinstalar los paquetes de software innecesarios

Si usted desactiva determinados servicios, también debería desinstalar los paquetes de software correspondientes. Así, asegura que esos servicios no supongan ningún peligro en el futuro, además de ahorrar valioso espacio de memoria. La instalación de software en los sistemas Linux está compuesta en su totalidad por paquetes modulares. Por lo tanto, bastará con identificar y desinstalar el paquete que ya no necesite. Esto también elimina automáticamente todas las dependencias, como pueden ser las entradas en los archivos de configuración. La administración de los paquetes de software bajo Linux es un tema muy extenso. Aquí sólo podemos dar unas breves nociones, centradas en la desinstalación de los paquetes que contengan servicios de Internet.

1. La instalación de paquetes entra dentro de las funciones de administración, que usted puede iniciar a través de herramientas de configuración como Yast2. Sólo resulta recomendable una desinstalación manual de los paquetes si usted conoce bien el paquete correspondiente y sabe eliminar manualmente todos los vínculos que tenga con otros componentes. En Yast2 encontrará la administración de paquetes en el menú principal, bajo el punto *Instalar/Desinstalar paquetes*. Actívela con el botón *Ejecutar módulo*. Tenga en cuenta que para la administración de los paquetes de software necesitará los CD-ROMs de la distribución.

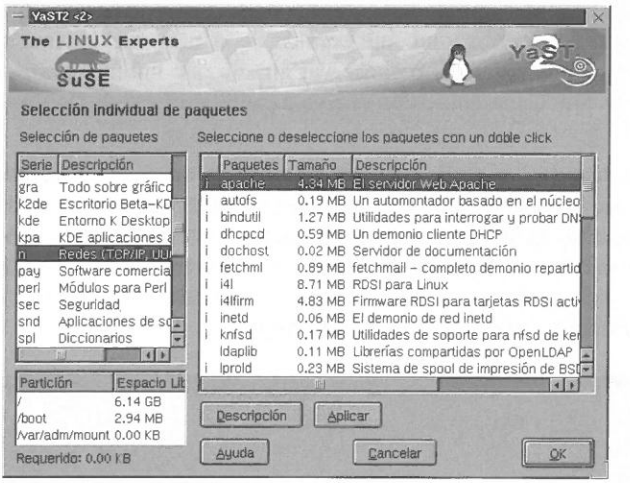


En los sistemas SuSE, encontrará la administración de paquetes de software como punto de selección en el menú principal de Yast2.

2. En el módulo de paquetes encontrará en primer lugar una relación de todos los paquetes de software que pertenezcan al volumen de la distribución. Por consiguiente, el menú visualizará tanto los paquetes instalados en ese momento, como los que aún puede instalar. Más adelante explicaremos cómo distinguir unos de otros.

3. En el apartado *Selección de paquetes*, situado en la parte superior izquierda, puede elegir en primer lugar la serie de paquetes que componen su instalación. Para hacer más fácil la administración, los numerosos paquetes van agrupados en series que suelen incluir paquetes de software del mismo ámbito de funciones. Por ejemplo, la serie *kde* contiene todos los paquetes que pertenezcan al escritorio KDE. Si elige una serie, en el área situado a la derecha de ésta aparecerá la lista de los paquetes de software de dicha serie.

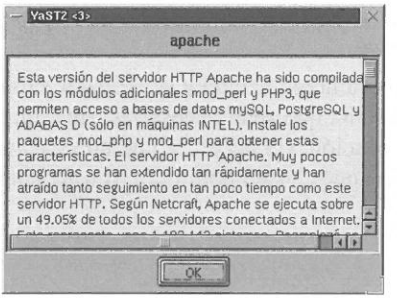
4. Para los servicios de Internet resulta especialmente interesante la serie *n*, que contiene la mayor parte de los servidores y servicios de Internet. Seleccione esa serie para que sean visualizados los correspondientes paquetes de software.



Seleccione la serie n para que sea visualizada la lista de paquetes de software de Internet.

5. En la lista de paquetes podrá reconocer por el signo de admiración inverso que precede a las diferentes entradas, que esos paquetes están instalados en ese momento. Las entradas sin ese signo forman parte de la distribución, pero no están instaladas. Por cierto, el hecho de que un paquete de software esté instalado no significa que también esté activado. Sólo quiere decir que el ordenador dispone de él y se puede activar en cualquier momento la funcionalidad correspondiente.

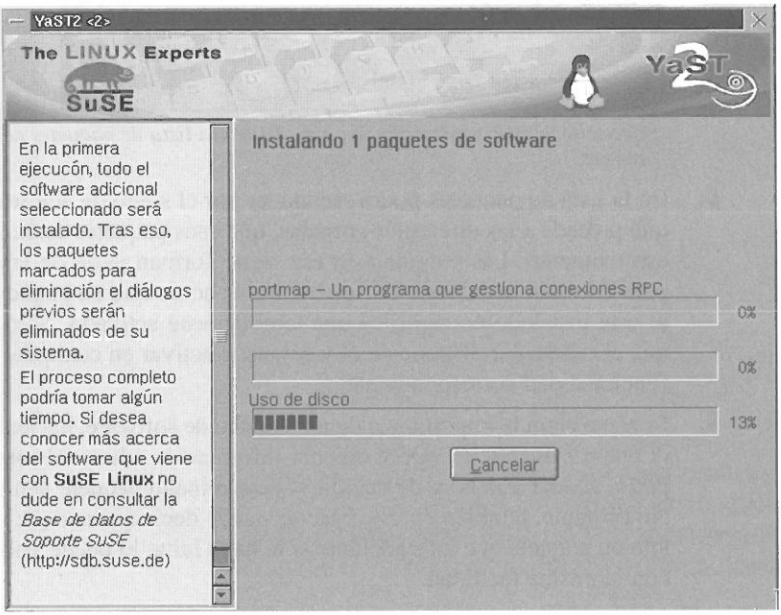
6. Si no ve clara la importancia de un paquete de software, haciendo clic sobre el botón *Descripción* podrá obtener información adicional sobre él. Ésta le podrá ayudar a la hora de decidir si determinado paquete aún es necesario. No obstante, también en este caso se puede decir que aunque usted desinstale un paquete que más adelante sí le haga falta, lo puede volver a instalar con la misma facilidad.



La breve descripción de los paquetes de software puede servirle de ayuda en caso de duda.

7. Para desinstalar uno de los paquetes de software, basta con hacer un doble clic sobre la correspondiente entrada de la lista. Del mismo modo, puede instalar otros paquetes o conservar alguno que hubiera destinado a la desinstalación. Cada doble clic vuelve a cambiar el estado del paquete de software.

8. Sólo cuando haga clic sobre el botón *OK*, ocurrirá de verdad algo. Será entonces cuando entren en vigor las modificaciones que usted haya definido anteriormente. Es decir, los paquetes correspondientes serán instalados o desinstalados. Esto puede llevar algún tiempo en función del alcance de las modificaciones. Mientras dure el proceso, una ventana de estado le informará mediante una barra de progreso.



En función de su alcance, la instalación o desinstalación de los paquetes de software puede llevar algún tiempo.

Cuando se ponen en práctica los cambios, también se realizan automáticamente todas las modificaciones del sistema que sean necesarias. En Linux esto puede hacerse durante el tiempo de ejecución, sin necesidad de un rearranque completo, como sucede en Windows. Después, usted podrá seguir trabajando con el sistema modificado.

¡Basta de jergas! – el vocabulario del hacker

El tema de los hackers viene rodeado de un sinfín de expresiones técnicas, abreviaturas y extrañas composiciones de palabras. Nosotros seguramente habremos empleado algunas en este libro, aunque siempre hemos procurado explicarlas in situ de manera fácilmente comprensible. Pero, por si acaso, para concluir el libro volvemos a resumir las expresiones más importantes en relación con este tema, con intención de definirlas de forma breve y concisa.

ActiveX

ActiveX es una tecnología desarrollada por Microsoft para hacer la competencia a -> Java. Permite integrar aplicaciones en páginas web. Los programas ActiveX pueden ser creados, por ejemplo, con VisualBasic. En contraste con Java, ActiveX no es independiente de plataformas y no posee un concepto de seguridad convincente. Por eso, generalmente se recomienda recurrir a las configuraciones de seguridad de Internet Explorer, para impedir la ejecución de los elementos ActiveX. Otros navegadores ni siquiera ejecutan los componentes ActiveX.

Acceso de sólo lectura

El derecho concedido a un usuario para ver el contenido de un directorio o un archivo. Quien posee este derecho, puede visualizar los archivos contenidos en un directorio. En cuanto a un archivo, el *derecho de lectura* permite abrir y ver su contenido. Para poder cambiar el contenido también, se requiere además el -> derecho de escritura.

Administrator

El *Administrator* es el administrador de un sistema, pudiéndose entender por sistema tanto un ordenador individual como una red completa. El administrador es responsable de que todo se desarrolle sin problemas y con seguridad. Da de alta a los usuarios, adjudica los derechos de acceso, se encarga de la instalación del software y mantiene todo el sistema.

Agujero de seguridad

Este es el nombre que recibe, independientemente de software o hardware, un punto débil en un sistema que permite funciones que en realidad no deberían consentirse, o bien facilita a personas no autorizadas el acceso a datos o funcio-

nes. Los agujeros de seguridad pueden deberse a errores de programa o de diseño, o también a configuraciones incorrectas.

Alias

Un *alias* es un nombre o concepto fácil de memorizar, que se emplea en lugar de otro nombre o concepto más largo o no tan fácil de recordar. Alias son, por ejemplo, los nombres IRC, pero también lo pueden ser las direcciones de correo electrónico.

ANSI

El ***American National Standards Institute*** es una entidad de estandarización de los Estados Unidos, comparable al Instituto DIN en Alemania. Lo más conocido es el código de caracteres llamado también ANSI, que define para la totalidad de los caracteres estándar unos códigos numéricos concretos vigentes en todos los sistemas informáticos. Esto hace que los mensajes de texto sean intercambiables entre diferentes sistemas operativos y plataformas de hardware, lo que supone una condición fundamental para el funcionamiento de Internet.

AOL

America Online es uno de los servicios online más importantes. Surgido originalmente en los Estados Unidos, AOL también trabaja desde hace algún tiempo a nivel internacional, por ejemplo en Europa. Este servicio tiene en todo el mundo más de 10 millones de abonados.

Applet

Un *Applet* es un pequeño programa especial que cumple una finalidad muy concreta. Por lo general, es empleado como componente de una página web, por ejemplo como asistente de navegación. Un programa más extenso y variado suele recibir el nombre de aplicación y es ejecutado aparte, fuera del –> navegador. Aunque a veces, las fronteras entre applet y aplicación son algo difusas. El término applet se emplea sobre todo en relación con Java-Applets.

ASCII

La ***American Standard Code for Information Interchange*** es una tabla de caracteres que asigna a todos los caracteres importantes un código numérico. Según este código, en todos los ordenadores del mundo a la "A" mayúscula le corresponde el número ASCII 65, para la "a" minúscula se emplea el 97. En contraste con ANSI, ASCII no sólo conoce los signos empleados en los Estados Unidos, sino también muchos caracteres especiales internacionales, como por ejemplo las vocales alemanas con diéresis o la eñe (ñ).

Auditoría

Se trata de una comprobación de la seguridad de un sistema, o de la aptitud de las medidas de seguridad. Puede ser realizada por una entidad independiente, o por el propio -> administrador responsable. Ayuda a analizar el estado de seguridad de un sistema y a descubrir los puntos débiles. En los sistemas críticos se deberían realizar auditorías a intervalos regulares, al margen de las demás medidas de seguridad.

Autentificación

Al comienzo de cualquier tipo de comunicación confidencial, los implicados deben verificar con quién están tratando y si el otro es realmente la persona que pretende ser. Para eso se hace una autentificación, en la que las partes se presentan y acreditan su identidad. Si un usuario humano quiere iniciar una sesión con un servicio, la autentificación casi siempre se hace con nombre de usuario y contraseña. Cuando la comunicación es entre máquinas, se intercambian y verifican con frecuencia las firmas.

Backup

Es recomendable hacer a intervalos regulares de tiempo copias de seguridad de los datos o archivos importantes. Si después se perdieran los datos a causa de un ataque o cualquier otra anomalía, se podría recuperar esa copia denominada como *Backup*, para restaurar al menos el estado de creación. De no haber ningún backup, los datos pueden perderse completamente y deberán ser generados de nuevo.

Bug

Bug se emplea normalmente para referirse a errores de programación. Cuando los primeros ordenadores de los años 40 sólo estaban compuestos por relés electrónicos, las fuentes de error más frecuentes eran las chinches (en inglés *bugs*), que se extraviaban en los relés y los bloqueaban. Desde entonces, se emplea ese nombre para hablar generalmente de un error en los programas.

Caché

Caché es la denominación general de una memoria intermedia, en la que se almacenan los datos empleados recientemente, para poder acceder pronto a ellos si hacen falta. Se emplean cachés en varios puntos, por ejemplo en el propio procesador o en el archivo de intercambio del sistema operativo. En el navegador web, la caché de Internet evita tener que repetir innecesariamente las transmisiones y acelera un nuevo acceso a páginas recién visitadas.

Certificado

Es una certificación electrónica con la que un usuario o un ordenador pueden acreditar su identidad ante otros.

CGI

La *Common Gateway Interface* (CGI) permite seguir procesando los datos introducidos por los usuarios en los formularios web, utilizando casi cualquier programa. Para ello, define una interfase, a través de la que se pueden transmitir datos de entrada a programas y scripts CGI y enviar la respuesta de vuelta a los usuarios.

Cliente

Cliente es la denominación que recibe un ordenador o programa, que a través de una red (por ejemplo Internet) solicita datos a un servidor y los transmite. Un navegador web es un cliente web, que solicita al servidor web documentos y datos, los recibe y a continuación los visualiza en la pantalla.

Compilador

Un *compilador* es un programa que convierte el código fuente de un lenguaje de programación (por ejemplo un listado C) en un programa ejecutable en lenguaje máquina. En la compilación, el programa es traducido totalmente antes de la pasada. El archivo binario resultante puede ser ejecutado sólo en ordenadores compatibles. En contraste con esto, los -> intérpretes no traducen los comandos del programa hasta el momento de la ejecución. Son más lentos, pero a cambio pueden ejecutarse casi siempre en diferentes plataformas.

CompuServe

CompuServe es uno de los servicios online más antiguos. Actualmente es propiedad de -> AOL, aunque sigue funcionando como servicio independiente. Dirige sus páginas, sobre todo, a personas dedicadas a los negocios y a científicos, aunque también tiene algo que ofrecer a los internautas normales. Además, facilita a sus clientes un acceso de calidad a Internet.

Contraseña de uso único

Es una contraseña generada dinámicamente para una transmisión de datos segura entre dos sistemas. Es acordada durante la autentificación y únicamente sirve mientras dure el intercambio de datos. Después caduca automáticamente. Las contraseñas de uso único son muy seguras, pero sólo pueden ser empleadas para la comunicación entre máquinas.

Control de acceso biométrico

Por regla general, el control de acceso para usuarios hoy en día aún se hace con identificador de usuario y contraseña. Estos métodos tienen sus debilidades conocidas. En el futuro, se aplicarán cada vez más controles biométricos. Éstos consisten en medir las características biológicas de una persona, como por ejemplo sus huellas dactilares, una muestra de su voz o su retina, o incluso el ADN. Actualmente ya hay escáneres de huellas dactilares, que permiten controlar el acceso a un PC.

Cookies

Las *cookies* son pequeños paquetes de datos que los servidores web pueden depositar en los ordenadores de sus visitantes. Sirven para reconocer a los usuarios si hacen una nueva visita. También los emplean las tiendas virtuales para administrar las cestas de la compra. Un desagradable efecto secundario de esta técnica es que las acciones de los usuarios pueden ser fácilmente rastreadas y espiadas valiéndose de las cookies. Por esta razón, en la mayoría de los navegadores web se puede restringir o impedir del todo la aceptación de cookies.

Correo electrónico (E-Mail)

El *e-mail* es el correo electrónico que se tramita a través de Internet o de servicios online. Para el e-mail se necesita un programa de correo electrónico y un buzón de correo electrónico con su correspondiente dirección.

Crack

Un programa o una técnica para reventar los dispositivos de seguridad. Por ejemplo, burlar las peticiones de contraseña, espiar contraseñas o descifrar encriptaciones.

Criptografía

La *criptografía* es la ciencia que se dedica a la encriptación de datos mediante procedimientos matemáticos.

Daemon

El *daemon* es una expresión surgida originalmente del entorno Unix, que alude al servidor (a procesos del servidor). Hoy en día, ya se emplea generalmente como denominación de todo tipo de servidores (por ejemplo servidores web).

Denial of Service (DoS)

Técnicas de ataque que consisten en sobrecargar el sistema atacado mediante un sinfín de consultas, hasta que al final éste deniega sus servicios totalmente. Así

se pueden poner fuera de combate con eficacia servidores web, pero también subredes enteras. Los más efectivos son los ataques DoS repartidos, donde las consultas proceden de un sinfín de ordenadores con cuyo control se había hecho antes el hacker.

Derecho de escritura

Este derecho permite, a quien lo posea, modificar archivos y guardar de modo permanente las modificaciones. En algunos sistemas operativos, esto implica también el derecho a crear archivos nuevos. En otros, existe un derecho especial sólo para eso. Por lo general, el derecho de escritura es adjudicado al mismo tiempo que el -> *derecho de lectura*.

Dirección IP

La *dirección IP* es la denominación inequívoca de un ordenador de Internet. Equivale al número IP y consta de cuatro partes, p.ej. *123.145.167.189*. Generalmente, las direcciones IP sólo son empleadas por ordenadores o programas. Las personas utilizan los -> nombres IP, que son más fáciles de recordar y mediante -> DNS pueden ser siempre convertidos en números IP.

DNS-Spoofing

Una técnica de hackers con la que se ataca a un sistema mediante -> datos DNS falsificados. Los datos pueden ser falsificados atacando al propio DNS o manipulando el circuito de transmisión de datos. Con esto se atrae al ordenador atacado hasta un servidor, al que toma por el verdadero, pero que en realidad es controlado por el hacker. Una técnica similar es -> IP-Spoofing.

Domain Name Service (DNS)

El *Domain Name Service* convierte a los nombres IP (por ejemplo www.server.com) en números IP (por ejemplo *123.145.167.189*), que corresponden a las verdaderas direcciones IP numéricas de los ordenadores de Internet. DNS también se emplea frecuentemente como abreviatura de Domain Name Server, el ordenador que realiza esta asignación. En algunos proveedores, hay que introducir manualmente el Domain Name Server en las -> configuraciones TCP/IP. Pero la mayoría de las veces, es transmitido automáticamente cuando se establece la conexión telefónica.

E-Mail anónimo

Si se enmascara la dirección del remitente, se pueden enviar anónimamente -> mensajes de correo electrónico. Para ello, los mensajes son dirigidos a través de un anonymizer, que elimina la dirección original del remitente y la sustituye por

una información que no dice nada. De este modo, es posible participar en grupos de debate sin tener que dar la cara. Por desgracia, este servicio también es empleado constantemente para fines ilícitos.

Encriptación asimétrica

Esto corresponde a un sistema de encriptación, en el que remitente y destinatario emplean claves distintas (asimétricas). Hay siempre una clave privada y una pública, pudiendo ser ésta última divulgada o transmitida a otros sin ningún problema. Esto resuelve el inconveniente que surge a la hora de transmitir la clave común. La aplicación más conocida es -> ***Pretty Good Privacy*** (PGP).

Entidad certificadora

Una organización o empresa que concede -> certificados. Por lo general, también define los requisitos que deben cumplir los propietarios de los certificados y vigila el cumplimiento de los mismos. Si se recibe un certificado para comprobación, siempre habría que verificar también la entidad certificadora que otorgó ese certificado. Un certificado sólo es tan digno de confianza como lo sea la organización que lo concedió.

Extranet

Al enlazar varios -> intranets mediante conexiones de Internet, se obtiene una *extranet*. Para los usuarios no tiene ninguna importancia si los datos requeridos proceden de la propia intranet o de otra. Las aplicaciones estándar son empresas que trabajan a escala mundial y enlazan diferentes redes regionales para formar una red virtual mundial.

Archivos log

Se denomina como *archivos log* a los archivos de protocolo que registran actividades, accesos, inicios de sesión, etc. que han tenido lugar en un ordenador. Los programas más variados los generan por los motivos más diversos. Los ordenadores de Internet muchas veces crean archivos log por razones de seguridad. Así, en un momento posterior se puede comprobar quién se conectó a una hora determinada y qué hizo.

File Transfer Protocol (FTP)

El ***File Transfer Protocol*** (FTP) es, en resumidas cuentas, uno de los protocolos de Internet más antiguos. Permite la transmisión de archivos a través de Internet. Los servidores FTP facilitan archivos de software, de los que los usuarios pueden descargar archivos. Para el acceso se necesitaba antiguamente un cliente FTP especial. Pero hoy en día, la mayoría de navegadores web modernos ya ofrecen dicha función.

Firewall

Un *firewall* es una barrera de seguridad electrónica que, por ejemplo, debe proteger una intranet de empresa contra el espionaje y el sabotaje. El nombre se deriva de los muros cortafuegos, que se construyen entre las casas para evitar que, en caso de incendio, las llamas pasen de una a otra. Según este principio, los firewalls criban el tráfico de datos para excluir de él los paquetes de datos que puedan ser dañinos. Aunque con esto, es posible que determinadas páginas y ciertos servicios de Internet ya no puedan ser usados en una intranet. Los firewalls pueden ser de software o de hardware.

Formularios

Los *formularios* son elementos interactivos de páginas web que permiten a los usuarios introducir datos o hacer selecciones. Pueden ser empleados para los fines más diversos (por ejemplo para darse de alta, hacer encuestas, tiendas virtuales, indicar la dirección, etc.). Generalmente, los datos introducidos en los formularios son tramitados por programas CGI.

Frequently Asked Questions (FAQ)

Frequently Asked Questions significa en español "preguntas hechas con frecuencia". Las FAQs son una lista de preguntas que se plantean regularmente sobre determinado tema. Normalmente, suelen ser contestadas enseguida dentro de una FAQ. En un principio, las FAQs surgieron de los grupos de noticias. Hoy en día, la idea también ha sido adaptada a otros entornos. Ya hay incluso FAQs que no tienen nada que ver con ordenadores.

Gateway

Se denomina como *gateway* a una transición entre diferentes protocolos. Así hay por ejemplo gateways entre Internet y los servicios online como -> AOL, para que los miembros de AOL puedan utilizar los servicios de Internet y estén localizables por correo electrónico. Por otro lado, -> CGI es un gateway que crea una interfase entre un -> servidor web y cualquier otro programa.

Grupo de noticias

Un *grupo de noticias* es una especie de tablón de anuncios digital en Internet, dedicado a un tema concreto. Cualquiera puede leer una noticia y redactar sus propios comunicados. Los grupos de noticias en todo el mundo son varias decenas de miles, por lo que es posible encontrar información y hacer preguntas sobre casi cualquier tema. Para leer los grupos de noticias se necesita un lector de noticias. Aunque esta función la proporcionan a veces los paquetes de los navegadores web actuales.

Gusano de Internet

Una variante especial de virus informático, que se propaga por sí sólo – es decir, sin que los usuarios intercambien conscientemente datos - a lo largo de una red. Para pasar de un ordenador a otro, suele aprovechar los agujeros de seguridad en software de amplia difusión. El ejemplo más conocido es el gusano Morris, que en noviembre de 1988 se extendió en 24 horas por todo Internet.

Hipertexto

Denominamos como documentos de *hipertexto* a los textos electrónicos que contienen referencias – también electrónicas – a otros documentos o partes de documentos. El ejemplo más conocido de hipertexto son las páginas web que incluyen links a otras páginas. Otro ejemplo popular son los archivos de ayuda de Windows.

Host

Host, que se podría traducir como "anfitrión", es otra expresión para -> servidor.

HTML

El ***Hypertext Markup Language*** (HTML) es un lenguaje de descripción de páginas para confeccionar páginas web. Contiene comandos llamados *tags*, que actúan sobre el layout del documento o sobre determinadas partes del mismo.

HTTP

El ***Hypertext Transfer Protocol*** (HTTP) es el protocolo de transmisión para páginas web. Define cómo pueden solicitar los navegadores web documentos y cómo los -> servidores web responden a estas peticiones.

Interface

Interface significa "interfase" en español. Por su función, las interfaces pueden ser comparadas con los -> gateways, aunque casi siempre se emplea esta expresión en un sentido más técnico (por ejemplo, haciendo referencia al hardware). Una interface es, por ejemplo, la interfaz paralela a la que se conecta la impresora en un PC.

Internet Service Provider (ISP)

El *Internet Service Provider* (ISP), llamado también proveedor de Internet o simplemente proveedor, facilita el acceso a Internet. A los usuarios privados les proporciona nodos de conexión telefónica para -> módem o -> RDSI. Los proveedores puros se diferencian de los servicios online, que aparte del acceso a Internet también ofrecen otros servicios.

Intérprete

Un *intérprete* es un programa que traduce, durante el tiempo de ejecución, el código fuente o código byte de un lenguaje de programación. Los programas interpretadores suelen ser casi siempre lentos. A cambio, el código fuente o código byte con frecuencia es independiente de plataformas, es decir, puede ser ejecutado en diversos ordenadores (PC, Mac, UNIX, etc.). Sólo el intérprete en sí debe ser específico para cada hardware. En contraste con esto, los -> compiladores casi siempre generan programas específicos para cada hardware. Los Java-Applets, por ejemplo, son ejecutados frecuentemente por intérpretes. Otro ejemplo puede ser JavaScript o Perl.

Intranet

Una *intranet* es una pequeña red cerrada en sí misma (por ejemplo, la red de una empresa), en la que se emplean las mismas técnicas, idénticos protocolos y programas que en Internet. Frente a las redes de empresa clásicas, las intranets ofrecen la ventaja de emplear una tecnología de amplia difusión, que por lo tanto es bien conocida y polifacética. Además, es muy fácil crear conexiones con Internet. A través de Internet se pueden agrupar varias intranets, para formar una -> extranet.

IP

El ***Internet Protocol*** (IP) es responsable de que los paquetes de datos lleguen al destino previsto. Junto con -> TCP, se encarga de descomponer, transmitir y recomponer los datos. Para ello emplea -> nombres IP o números IP, que identifican de modo inequívoco a remitentes y destinatarios.

IP-Spoofing

Método de ataque donde, de modo similar al -> DNS-Spoofing, el atacante simula la dirección IP de otro ordenador. Así puede hacerse con acceso a sistemas, en los que la -> autentificación se base en la dirección IP.

IRC

Internet Relay Chat es una red de servidores, a través de la cual pueden comunicarse los chatters de todo el mundo. Para eso se necesita un cliente IRC. La comunicación transcurre a través de canales donde se reúnen los chatters que compartan un interés concreto. Aparte de esto, IRC también facilita funciones para la comunicación privada y para el intercambio de archivos.

Java

Java es el lenguaje de programación de Internet. Es – como la misma Red –

independiente de plataformas, de modo que un programa ya escrito puede funcionar en casi todas las plataformas de ordenador. Para ejecutar un programa Java se requiere una máquina virtual de Java, incluida por ejemplo en el equipamiento integral de Internet Explorer.

JavaScript

Este lenguaje script para páginas web sólo se asemeja a -> Java en el nombre. De hecho, fue desarrollado por la empresa Netscape para dar a las páginas web una forma más dinámica e interactiva. Todos los navegadores web actuales soportan componentes JavaScript. Aunque como contenido activo que es, JavaScript entraña algunos riesgos.

LAN

Local Area Network (LAN) es una red local de ordenadores. Su aplicación más frecuente es en redes de empresa, donde todos los ordenadores de una empresa están interconectados para compartir recursos o facilitar la información en toda la compañía. Las LANs en las que los ordenadores se comunican con -> TCP/IP, son denominadas también como -> intranets. A partir de determinada distancia entre los ordenadores, la LAN se convierte en Wide Area Network (WAN). Aunque la frontera entre una y otra aún no ha sido definida con exactitud.

Listas de correo

Las *listas de correo* son direcciones de distribución utilizadas para remitir un -> mensaje de e-mail a muchos destinatarios. Son administradas en servidores de listas y generalmente, están dedicadas a un tema concreto. Se distingue entre listas de mensajes que sólo se emplean para avisar a los suscriptores y listas de debate, donde los suscriptores pueden comunicarse entre sí.

MIME

Los ***Multipurpose Internet Mail Extensions*** (MIME) complementan el -> estándar de correo electrónico SMTP y eliminan algunas de sus debilidades e insuficiencias. Por ejemplo, MIME permite emplear en un e-mail todas las vocales con diéresis que se desee.

Módem

Modem es la abreviatura de modulator-demodulator – un aparato que convierte la información digital en señales analógicas, que pueden ser enviadas a través de una línea telefónica analógica. Al otro extremo, otro módem tiene que convertir de nuevo las señales analógicas en información digital. Los módems actuales trabajan con una capacidad de 56 KBit/s y más.

Navegador

Un *navegador* es un programa para visualizar determinados contenidos. Casi siempre se refiere a los navegadores web que permiten ver páginas web. Ejemplos conocidos de navegadores web son Internet Explorer, -> Netscape Navigator y recientemente Opera.

NCSA

El *National Center for Supercomputing Applications* (NCSA) ha sobresalido especialmente en el desarrollo de software para Internet. Allí nació el popular navegador web Mosaic, a partir del cual se desarrolló Netscape Navigator. Aún goza de amplia difusión el servidor web NCSA.

Netiquette

Esta palabra artificial, compuesta de *net* (en español "red") y *etiquette* (en español "etiqueta"), se refiere a las reglas de juego genéricas para relacionarse con otros usuarios de Internet y manejar los recursos de la Red. A rasgos generales, se basa en el sentido común y en algunas reglas no escritas. Para determinados servicios, grupos y foros hay acuerdos escritos en forma de -> FAQs.

Netscape Navigator

Netscape Navigator es el segundo navegador web más importante, además de Internet Explorer. Tras haber perdido el Navigator en los últimos años bastante terreno en el mercado, la empresa Netscape publicó el código fuente y cerró alianzas estratégicas con las empresas Sun y AOL. El primer resultado fue Netscape 6, publicado a finales del año 2000. En cuestión de alcance y calidad de sus funciones, Netscape Navigator e Internet Explorer presentan muy pocas diferencias. Aunque hasta la fecha, Microsoft lleva la delantera en estrategia y marketing.

Nombres IP

Los *nombres IP* son la denominación textual de las direcciones de Internet (p.ej. www.server.com). Pueden ser representados tanto por -> DNS como por direcciones IP o números IP específicos.

NSA

La *National Security Agency* es uno de los servicios secretos más importantes de los Estados Unidos, responsable de proteger todos los sistemas de seguridad que tengan importancia para la nación. Por lo tanto, la NSA se dedica de forma intensiva a la -> criptografía, los ataques de escucha y todas las variantes de espionaje técnico. Hay más información al respecto bajo http://www.nsa.org.

Online

Mientras el ordenador mantenga una conexión activa con otro PC o con una red (es decir, mientras haya datos transitando de acá para allá), estará *online* (en español: "en línea"). Cuando la conexión sea interrumpida, se retirará de la línea y estará *offline*.

Patch

En realidad, el software nunca está libre de errores. Muchas veces no se trata más que de pequeñas deficiencias que apenas molestan a nadie, o que sólo aparecen en determinadas situaciones infrecuentes. Pero a veces, en aplicaciones complejas se manifiestan también errores graves, que perjudican a funciones importantes o suponen riesgos para la seguridad. En estos casos, el fabricante reacciona (o al menos, eso esperamos todos) con un programa de reparación que subsane ese error. Este retoque de una o varias funciones concretas recibe el nombre de patch o parche.

Perl

Practical Extraction and Reporting Language es un lenguaje script empleado con frecuencia en entornos de red. Su fuerza especial está en que pone claridad en las grandes cantidades de datos. Sobre todo en el entorno -> UNIX, es apreciado tanto por -> administradores como por hackers, para analizar, por ejemplo, los -> archivos log y las listas de directorios.

PGP

Pretty Good Privacy (PGP) es un programa para encriptar e-mails y otros datos. Es un freeware gratuito de gran popularidad y amplia difusión en Internet. Hay una versión especial para Windows, que puede ser descargada bajo la dirección http://www.pgpi.com. Ésta incluye un plug-in especial para Outlook Express y para otros programas de correo electrónico, que integra las funciones PGP en la propia interfaz de los programas.

Plug-in

Un *plug-in* es en términos generales un módulo de ampliación para una aplicación, que facilita a éstas funciones adicionales. Hay una amplia serie de plug-ins para navegadores web, que permiten representar y procesar formatos de datos multimedia que el navegador de origen no es capaz de manejar.

PPP

Point-to-Point-Protocol (PPP) es un procedimiento para transmitir datos a través de líneas telefónicas analógicas. Se emplea cuando los usuarios se conectan

telefónicamente vía módem a su proveedor de Internet. Hoy en día, PPP ha sustituido a su predecesor -> SLIP en casi todas partes.

Public Key

Public Key es la denominación que recibe la clave pública en un -> sistema de encriptación asimétrico, como por ejemplo -> PGP. La clave pública puede ser distribuida a los demás tranquilamente a través de Internet, ya que no permite sacar conclusiones sobre la clave privada (-> *Secret Key*).

Puerta trasera

Una entrada clandestina a un sistema, que permite el acceso burlando las medidas de seguridad habituales. Muchas veces, los programadores dejan, por comodidad, puertas traseras en sus productos, que con el tiempo son detectadas y aprovechadas por los hackers. También se pueden crear activamente puertas traseras, por ejemplo empleando -> troyanos.

RDSI

Integrated Services Digital Network (ISDN) es el estándar para telefonía digital. Para telefonear aporta una calidad vocal digital y muchas prestaciones cómodas. A los usuarios de Internet les posibilita unos accesos a la Red sin problemas, de hasta 64 KBit/s y más.

Red privada virtual (RPV)

Una técnica en la que ordenadores individuales o redes son enlazados a través de Internet para formar una red común. Aquí, las transmisiones de datos a través de Internet se desarrollan de forma transparente (es decir, imperceptible para el usuario) y son encriptadas, de modo que dentro de la red virtual quede garantizada la confidencialidad e integridad de los datos.

Requests for Comments (RFCs)

Request for Comments (RFCs) son documentos que definen tecnologías y protocolos para Internet. Son considerados universalmente como estándares de Internet. Quién esté interesado en técnicas e interioridades, podrá descargar estos textos de muchos servidores FTP.

Routing/Router

Se denomina como *routing* al arte de direccionar los datos en Internet. Y es que en una red de tanta complejidad, no resulta precisamente fácil encontrar siempre la ruta más apropiada. A fin de cuentas, ésta no depende sólo de la comunicación geográficamente más corta, sino también de las capacidades transmisivas de los

diferentes trechos y del grado de ocupación en cada momento. Los routers son las centrales de tráfico de Internet y se encargan de las tareas correspondientes.

RSA

RSA es un algoritmo de encriptación -> asimétrica, que recibió este nombre por sus creadores Rivest, Shamir y Adleman. Está entre los procedimientos de encriptación más usados y se emplea en muchos productos. Su fiabilidad depende del tamaño de la clave. Las claves de hasta 40 Bit ya han sido atacadas con éxito. Pero las longitudes de clave de hasta 128 Bit, habituales hoy en día, sólo pueden ser reventadas con un enorme esfuerzo aritmético. Salvo que alguien haya encontrado secretamente un procedimiento para burlar al RSA.

SATAN

La *Security Administrators Tool für Analyzing* Networks es una herramienta tristemente celebre. Es capaz de analizar los ordenadores a través de la red y descubre sin piedad errores de configuración y agujeros de seguridad. En realidad iba destinada a los administradores de sistemas, para que verificaran a fondo los propios sistemas. Pero los hackers la emplean con la misma frecuencia y devoción para averiguar los puntos de ataque de sus víctimas.

Secret Key

Secret Key es la denominación que recibe la clave privada en un sistema de encriptación -> asimétrica, como por ejemplo -> PGP. La clave privada suele estar protegida por contraseña, de modo que sólo la puede emplear su legítimo propietario. Aun así, se debe vigilar muy bien la Secret Key.

Service Pack

Un *Service Pack* es un archivo de actualización para un programa, que corrige errores o incluye funciones nuevas o bien adapta el programa a las nuevas tecnologías. En contraste con un patch, que se centra siempre en un problema muy concreto, un Service Pack incluye un gran número de actualizaciones. También hay Service Packs para navegadores web, como por ejemplo Internet Explorer. Los Service Packs son especialmente importantes en sistemas operativos como Windows NT.

Servidor

En términos generales, un *servidor* es un ordenador que suministra información en una red. Los clientes pueden iniciar sesión con el servidor y descargar esa información. En Internet hay una amplia serie de servidores, como por ejemplo -> servidores web, -> servidores FTP, ->servidores de correo, -> servidores IRC o servidores de directorios.

Servidor de correo

Los *servidores de correo* son responsables de distribuir el correo electrónico (-> e-mail) en Internet. Se establece una distinción entre servidores de entrada de correo y *servidores de salida de correo*. Los servidores de entrada de correo (llamados también servidores POP o IMAP) almacenan los mensajes recibidos hasta que el destinatario los recoja con su programa de e-mail. *Los servidores de salida de correo* reciben los mensajes y los remiten al destinatario.

Servidor Proxy

Un *servidor Proxy* sirve para ahorrar capacidades de transmisión. Recibe las consultas de los clientes y las remite al verdadero servidor. Las respuestas del servidor a su vez van al servidor Proxy, que se las hace llegar al cliente. Al mismo tiempo, almacena una copia de los datos en su caché de Internet. Si en el futuro otros clientes solicitan los mismos datos, las consultas son contestadas directamente por el servidor Proxy, con lo que se acelera el proceso y se ahorran capacidades de transmisión. Muchos servidores online y proveedores de Internet emplean servidores Proxy para acelerarles a sus clientes el acceso, pero también para ahorrar ellos mismos dinero.

Servidor web

Un *servidor web* es un servidor especial que pone a disposición páginas web. Los navegadores web pueden establecer una conexión con el servidor web y solicitarle páginas web, imágenes u otros componentes. El servidor responderá con los datos requeridos.

SET

Con las ***Secure Electronic Transactions*** (SET), usted puede pagar con toda tranquilidad utilizando su tarjeta de crédito a través de un procedimiento encriptado donde interviene un procesador que actúa de mediador entre el comprador y el vendedor. Así, el vendedor sólo obtiene los datos imprescindibles, con lo que quedan ampliamente excluidas las posibilidades de hacer uso ilícito de los mismos. Sin embargo, hasta la fecha SET sólo es soportado por relativamente pocos bancos, entidades de tarjetas de crédito y tiendas virtuales.

Shell

Esta es la expresión técnica inglesa que hace referencia a una consola de entrada, donde se pueden introducir los comandos directamente por teclado. El *shell* de Windows es la línea de comandos MS-DOS. Los sistemas UNIX como Linux también tienen shells, que en principio funcionan igual. Pero los de UNIX suelen ser más potentes y flexibles. Muchos hackers prefieren los shells, porque con

ellos – siempre que se conozcan bien los comandos necesarios – se trabaja más deprisa y con más flexibilidad. De todos modos, el acceso a través de una red a un sistema atacado, casi siempre, no es otra cosa que un shell. Así que deben conocerlos bien.

Shell-Script

Un *Shell-Script* es un archivo de texto que contiene una serie de comandos shell. Al ejecutar este archivo, también son cumplidos los comandos transmitiéndolos sucesivamente al shell. De este modo, se pueden automatizar, por ejemplo, procesos regulares. Los shell-scripts pueden ser comparados con los archivos batch, que quizá algún usuario de Windows conozca todavía de tiempos pasados.

S-HTTP

El *Secure-Hypertext Transfer Protokoll* (S-HTTP) es un perfeccionamiento del -> *Hypertext Transfer Protokoll* (HTTP). Contiene, sobre todo, funciones de seguridad para encriptar y para la comunicación confidencial con certificados.

Sistema de encriptación simétrica

En un *sistema de encriptación simétrica*, el remitente y el destinatario de un mensaje codificado emplean la misma clave para encriptar o desencriptar. El gran problema de este procedimiento es que antes de iniciar la verdadera comunicación hay que intercambiar la clave con la otra persona a través de una vía segura. Por razones de seguridad, para eso no debería emplearse el mismo camino por el que después serán intercambiados también los mensajes.

SLIP

El *Serial Line Internet Protocol* (SLIP) es el predecesor de -> PPP, que actualmente ya se emplea en casi todas partes. Comparado con PPP, es menos potente y no posee funciones para la corrección automática de errores. Si su proveedor aún utiliza SLIP, debería ir pensando en deshacerse de él o buscarse otro.

SMTP

El *Simple Mail Transfer Protocol* (SMTP) se emplea para transmitir -> correo electrónico a través de -> conexiones TCTP/IP. Este es el protocolo utilizado por los servidores de salida de correo para enviar los mensajes.

Sniffer

Un programa de vigilancia que registra y monitoriza en una red los datos enviados. Puede utilizarse, por ejemplo, para diagnosticar problemas en la red o para vigilar el tráfico de datos. Los hackers emplean los *sniffer* para averiguar los

identificadores de usuario y las contraseñas que se transmitan a través de la red. Todos los datos que se envíen a través de una red sin encriptar pueden ser espiados por un sniffer.

Social Engineering

Social Engineering, llamado también Social Hacking, describe los métodos de hackers que trabajan más allá de la técnica. En el engineering pasivo, se intenta recopilar la mayor cantidad de información posible sobre la víctima. Así, se pueden encontrar, por ejemplo, alusiones a contraseñas o analizar el comportamiento de una persona. En el engineering activo, lo que se hace es contactar directamente con la víctima e intentar sonsacarle información confidencial. El ejemplo más conocido podría ser la llamada de un supuesto técnico, que quiere saber la contraseña para poder comprobarla.

SSL

Secure Socket Layer (SSL) es un protocolo de seguridad para encriptar las transmisiones a través de la Red. SSL permite establecer conexiones seguras, donde todas las transmisiones vayan encriptadas. Suelen emplearse, por ejemplo, para pagar en las tiendas virtuales.

Suma de comprobación

Una suma de comprobación (denominada también como suma de chequeo) es un número relativamente pequeño, derivado de una gran masa de datos aplicando un procedimiento matemático concreto. Los antivirus, por ejemplo, generan sumas de comprobación de archivos. Estas son verificadas a intervalos regulares, es decir, se crea una nueva suma de comprobación del archivo y se la compara con la vieja. Si hay diferencias entre las dos, significará que el archivo ha cambiado y quizá pueda contener un virus. Si la nueva suma es igual que la anterior, el archivo tampoco habrá sufrido alteraciones.

TCP

El T***ransmission Control Protocol*** (TCP) vigila, junto con -> IP, que el transporte de datos en Internet se desarrolle sin problemas. Es responsable de descomponer en paquetes los datos a enviar. Cuando los paquetes llegan al destinatario, los recompone de nuevo.

TCP/IP

El protocolo de transmisión de Internet -> *TCP/IP* consta de dos elementos. -> TCP descompone los datos a transmitir en paquetes, que son enviados por -> IP. TCP los recibe y los vuelve a componer tal y como estaban.

Teletransmisión de datos

Se denomina como *teletransmisión de datos* al intercambio de datos entre dos ordenadores conectados entre sí a través de una línea de datos (por ejemplo línea telefónica y -> módem). Un tipo así de conexión de teletransmisión de datos es necesario, por ejemplo, para conectarse telefónicamente a un proveedor de Internet.

TEMPEST

La ***T**ransient **E**lectro**m**agnetic **P**ulse **E**manation **S**tandard **T**echnology* se encarga de interceptar para fines de espionaje la radiación electromagnética de los aparatos técnicos. De este modo, si se posee el equipo adecuado, la imagen de un monitor de ordenador puede ser visualizada incluso a una distancia de hasta cien metros. TEMPEST es la denominación que recibe el fenómeno de la radiación y también un estándar para aparatos que van protegidos especialmente contra esta radiación.

T-Online

T-Online es el servicio online alemán más importante, surgido del videotexto (BTX) de la Deutsche Telekom. Desde la privatización de la Telekom, T-Online es en teoría una empresa independiente, aunque las dos siguen trabajando en estrecha colaboración. Para el acceso a Internet, T-Online sigue empleando un winsocket propietario, por lo que sólo puede ser recomendado con reservas a los usuarios de Internet. Pero también se puede establecer una conexión directa a través de la red de teletransmisión de datos Windows, que es plenamente compatible.

Traceroute

Un programa del entorno TCP/IP, que rastrea y monitoriza la ruta que siguen los paquetes de datos desde el ordenador propio hasta el ordenador objetivo. Viene incluido en el volumen de suministro de la mayoría de sistemas operativos. La variante para Windows se llama *tracert*.

Troyano

Un *troyano* o caballo de Troya, es un software que finge realizar determinadas funciones, cuando en realidad (o adicionalmente) hace cosas totalmente diferentes y por lo general, dañinas. El nombre se remonta a la mitología griega, que narra cómo fue conquistada la ciudad de Troya con la ayuda de un caballo de madera hueco.

UDP

UDP significa ***User Datagram Protocol*** y, en contraste con -> TCP/IP, trabaja sin conexión. Esto quiere decir que no existe ninguna conexión fija entre dos ordenadores. Uno de ellos envía la información y supone que el otro la recibirá. Se emplea para transmisiones de datos como las audioconferencias o videoconferencias, donde la pérdida parcial de información no tiene una importancia decisiva. El protocolo UDP no incluye ninguna función para garantizar la corrección e integridad de los datos transmitidos. Si se desea asegurarlas, deberá encargarse de eso la propia aplicación.

Unix

Unix es un sistema operativo multiusuario y multitarea. Fue desarrollado ya a comienzos de los años setenta por AT&T. Hoy en día, esta denominación se aplica a una amplia serie de sistemas compatibles con UNIX y derivados afines a UNIX. A este ilustre círculo pertenece también el sistema operativo para PC Linux, que actualmente goza de gran popularidad. Casi siempre, el software de Unix se deja transferir con relativa rapidez a otro sistema o derivado. Muchos servidores de Internet trabajan bajo UNIX, por ser considerado este sistema como muy estable y seguro.

Usenet

La denominación *Usenet* se emplea casi siempre como sinónimo para el conjunto de todos los -> grupos de noticias del mundo. Pero en sentido estricto, se refiere a las redes que intercambian información a través del ***Unix-to-Unix-Copy-Protokoll*** (UUCP). Éstas son subredes enlazadas con Internet a través de -> gateways, que no ofrecen una comunicación en tiempo real sino sólo servicios diferidos, como las noticias y el -> correo electrónico.

Virus

Los *virus informáticos* son pequeños programas, casi siempre malignos, que se multiplican por sí mismos y pueden causar daños en los PCs infectados. Precisamente Internet sirve de vía de propagación para estos parásitos. Antes de bajarse archivos de Internet, usted debería instalar sin falta en su PC un software antivirus actualizado.

WWW

WWW, ***World Wide Web***, *W3* o simplemente *Web*, son las denominaciones que recibe el conjunto de todos los servidores web, o de la información que ofrecen. Según estimaciones actuales, hoy en día existen varios cientos de millones de páginas web y se supone que pronto se alcanzará el límite de los mil millones.

Glosario

!BIOS, ...74
007 Password Recovery, ...107

A

Absolute HTML Compressor, ...508
Accesos remotos, ...48
Active Setup, ...149
ActiveX, ...125, 153, 537
  Authenticode, ...153
  desactivar, ...154
Administrador, ...537
Administrador de usuarios, ...75
  activar, ...76
  burlar, ...84
  nuevos perfiles de usuario, ...79
  seguridad, ...82
ADSL, ...301
Agujeros de seguridad, ...45, 146
Alias, ...538
Alternativos, sistemas operativos, ...519
Ambito privado, ...126
America Online, ...538
Análisis de redes, ...27
Análisis del texto claro, ...403
Análisis del texto claro seleccionado, ...403
Análisis del texto clave, ...403
Anonimato, ...481
  cookies, ...465
  investigación sobre personas, ...454
  Private Idaho, ...366
  Stealth Anonymizer, ...490
Anónimo, ...90
  e-mail, ...542
Anonymizer, ...486
Anonymizer-Proxy, ...488
ANSI, ...538
AntiOnline, ...284
Anti-Trojan, ...185
AntiVir, ...173
AOL, ...538
Aplicaciones
  vigilancia, ...249
Applet, ...538
Archivo ZIP
  contraseña, ...112
Archivos de noticias, ...460
ASCII, ...538
Asimétrica, encriptación, ...399, 543
Asistente para perfiles, ...138
Atacantes
  combatirles, ...284
Ataques, ...19
  a homepages, ...497
  a servidores web, ...516
  accesos remotos, ...48
  agujeros de seguridad, ...45
  análisis del objetivo, ...24
  ataques por fuerza bruta, ...47
  Denial of Service, ...52
  elección del método, ...40
  en Internet, ...52
  fallos del sistema, ...45
  manipulaciones IP, ...54
  protolocarlos, ...249
  secuestro de conexiones, ...55
  Sniffing, ...51
  Social Hacking, ...56
  troyanos, ...42
  virus informáticos, ...41
Ataques a PCs en red, ...300
Ataques de hackers, ...19
Ataques por hardware, ...114
Auditoría, ...539
Autentificación, ...539
Authenticode, ...153
Award-BIOS, ...70

B

BackOrifice, ...43
Backup, ...539
Base de datos de registro, ...83
Basic Input Output System. .....Véase BIOS
Biométrica, ...541
BIOS, ...69
  !BIOS, ...74
  Award, ...70
  burlar la protección por contraseña, ...73
  configuración del teclado, ...70
  forzar el acceso, ...74
  Reset, ...73
BlackICE, ...310
  advICE, ...312
  niveles de seguridad, ...310
  reacciones ante las alarmas, ...312

testear, ...314
Bombas de correo, ...375
Bookmarks, ...328
Boot-Viren, ...171
Browsercheck, ...146
Brute Force, ...47, 403
Bug, ...539
Bugfixes, ...46
Buscadores, ...19, 454
metabúsqueda, ...455
Búsqueda de personas, ...21
Búsqueda por personas, ...21
Bytecode, ...156

C

Cabecera
datos, ...373
Cabecera Received, ...374
Cabecera X, ...374
Caché, ...539
Caché de Internet, ...327
Cajón de arena, ...193
Candados de disquetes, ...172
CaptureNet, ...316
analizar los datos, ...318
CD-ROMs, ...67
aviso de inserción automática, ...99
Certificado, ...540
generarlo, ...431
Certificados, ...136, 430
desencriptar, ...433
distribuir, ...432
encriptación y firma, ...433
CGI, ...540
chronicle, ...37
Chronicle, ...35
Cifra, ...403
Clave
distribuir, ...413
importar, ... 415
privada, ...399
pública, ...400
publicarla en el servidor de claves, ...413
Clave privada, ...399
Clave pública, ...400
Claves
distribución, ...401
forzarlas, ...402
uso paralelo, ...407
Cliente, ...540
Compilador, ...540
Complete Cleanup, ...337
CompuServe, ...540
Conexiones
seguras e inseguras, ...137, 140
Conexiones seguras, ...140, 446
Configuración del teclado, ...70
contenidos activos, ...125
Contenidos activos, ...152
Contramedidas, ...283
Contraseña, ...101
aplicaciones, ...111
aplicaciones Office, ...111
archivos ZIP, ...112
ataques por fuerza bruta, ...47
de uso único, ...540
documentos, ...111
elección segura, ...103
en el puesto de trabajo, ...338
espiarla, ...256
frase personal, ...103
guardarla con seguridad, ...339
longitud, ...104
ma_usculas/minúsculas, ...105
medidas inmediatas, ... 110
medidas precautorias, ...105
olvido, ...107
PassKeeper, ...339
proteger, ...105
salvapantallas, ...94
síntomas de que ha sido desencriptada, 109
Contraseña BIOS, ...70
Contraseñas
en diálogos de inicio de sesión, ...106
en freemailers, ...448
guardar, ...106
Cookie Pal, ...475
procesar los cookies, ...479
cookies, ...465
Cookies, ...541
comprobar su existencia, ...468
Cookie Pal, ...475
peligro, ...466
previa consulta, ...473
procesar, ...479
programación, ...467
Correo electrónico
anónimo, ...542
averiguar direcciones, ...458
bombas, ...375
cabecera, ...373
cabecera Received, ...374
cabecera X, ...374
como arma, ...365

confidencialidad, ...390
desencriptar mensajes, ...420
Echelon, ...364
Email Remover, ...377
encriptar, ...397
entradas de cabecera, ...373
entradas Received, ...392
espionaje, ...394
falsificaciones, ...370
firmar mensajes, ...421
freemailer, ...444
limpiar el apartado de correo, ... 377
list-linking, ...376
Private Idaho, ...366
proteger la dirección, ...144, 484
seguir la ruta, ...392
transporte, ... 390
verificar firmas, ...424
vigilancia, ...324
virus, ...381
Crack, ...541
Criptografía, ...402, 541

D

Daemon, ...541
Data Encryption Standard, ...398
Datos históricos
en los freemailer, ...447
De uso único, contraseña, ...540
Deja.com, ...21, 460
Denial of Service, ...52, 541
DENIC, ...273
DES, ...398
Detección de ataques, ...310
BlackICE, ...310
Diálogos de inicio de sesión
guardar contraseña, ...106
Diffie-Hellman/DSS, ...407
Dirección IP, ...542
Direcciones de correo electrónico, ...458
en homepages, ...499
Directrices de uso, ...326
Directrices para el sistema, ...75
Disquetes, ...67
DNS, ...29, 269, 542
DNS-Spoofing, ...542
Domain Name Service, ...269. Véase DNS

E

Echelon, ...364
EICAR, ...173
E-mail, ... 364, 541
hoax, ...389
reglas para freemailer, ...446
usar varias direcciones, ...448
Email Remover, ... 377
Emisores perturbadores, ...119
Encriptación, ... 397
asimétrica, ...399, 543
forzarla, ...402
PGP, ...404
S/MIME, ...432
simétrica, ...397, 553
Enlaces de los protocolos de red, ...355
Entidad certificadora, ...543
Entradas Received, ...392
eSafe, ...85, 221
administrador de usuarios, ...85
análisis manual del sistema, ...225
áreas sensibles, ...240
asignar usuario, ...89
asistente de configuración, ...229
cajón de arena, ...194
conjuntos de reglas en función del tiempo, 242
conjuntos de reglas para usuarios, .86, 244
conjuntos de reglas propios, ... 232
conjuntos de reglas ya definidos, ...230
crear usuario, ...89
definir filtros de puerto, ...233
filtrar paquetes de datos, ...237
filtro de contenido, ... 237
filtro de palabras clave, ...239
Firewall, ...221, 228
funciones de seguridad, ...248
informe resumido, ...92
instalar, ...222
modo de aprendizaje, ...197
modo de aviso, ... 88, 244
modo interactivo, ...198
monitor de seguridad, ...227
palabras prohibidas, ...238
panorámica, ...248
proteger datos confidenciales, ...240
protocolo, ...92
Sandbox, ...86, 194
símbolo de estado, ... 227
testear programas, ... 194
usuario anónimo, ...90
violaciones de las reglas, ... 200
Escáner antivirus
testear, ...173
Escáners de segundo plano, ...173
Espionaje económico, ...296

Esteganografía, ...434
fichero portador, ...437
Steganos, ...436
Excel
contraseña, ... 111
Exploraciones, ...19

F

Fallos del sistema, ...45
Falsificaciones
correo electrónico, ... 370
FAQ, ...544
Favoritos, ... 328
Fichero portador, ... 437
Ficheros de protocolo, ...543
Ficheros log, ...543
File Transfer Protocol. ....Véase FTP
Filtro de puerto, ...233
Firewall, ...544
Firewall Personal, ...207
modo de funcionamiento, ...205
soluciones profesionales, ...206
ZoneAlarm, ...207
Firewall personal, ...207
ZoneAlarm, ...207
Firewalls, ... 38
Firewalls personales, ...38, 159
Formularios, ...544
Fortezza, ...138
Freemailer, ...444
cerrar la sesión, ...446
conexiones seguras, ...446
contraseñas, ...448
datos históricos, ...447
reglas de seguridad, ...446
relación de proveedores, ... 445
FTP, ...32, 543
Función de historial, ...328

G

Gateway, ...25, 544
Georgi Guninski, ...148
Grinder, ...33, 37
Grupo de noticias, ...544
Guerra de la información, ...65
Gusano de Internet, ...545

H

Hacker, ...16
accesos remotos, ...48
aficionados, ...61
análisis de redes, ...27
análisis del objetivo, ...24
ataques por fuerza bruta, ...47
definiciones, ...58
delitos penales, ...295
elección del método de ataque, ... 40
en Internet, ...52
en la guerra de la información, ...65
espías, ... 64
exploraciones, ...19
ideólogos, ... 61
indemnización por daños y perjuicios, .296
obtención de la información, ...22
profesionales, ...64
puntos débiles, ...17
recursos legales contra, ...295
saboteadores, ... 64
Script-kids, ...59
Social Hacking, ...56
Troyanos, ... 42
Hacker profesional, ...64
Hackers
combatirles, ...284
hackers ocasionales, ...60
Hackers aficionados, ...61
Hackers ocasionales, ...60
HackerWatch, ...284
HackTracer, ...292
notificar ataques, ...292
HackTracer, ...286
falsas alarmas, ...294
HackerWatch, ...292
niveles de seguridad, ...287
protocolo de incidencias, ...293
rastrear a los atacantes, ...290
Hipertexto, ...545
Hoax, ...389
Homepages
áreas protegidas, ...514
como fuente de información, ...499
protección, ... 497
protegerlas, ...507
Host, ... 545
HTML, ...545
HTTP, ...204, 481, 545
https, ...135
Huellas de navegación, ...326
Complete Cleanup, ...337

I

ICMP, ...53

IDEA, ...399
IDS, ...310
BlackICE, ...310
Imágenes
uso fraudulento, ...510
Impresora, ...67
Indagación sobre personas
archivos de noticias, ...460
Deja.com, ...460
direcciones de correo electrónico, ...458
guía telefónica, ...463
Indemnización por daños y perjuicios, ...296
inetd, ...528
inetd.conf, ...532
Informaciones online, ...22
Information Warfare, ...65
Interceptar monitores, ...115
Interface, ...545
International Data Encryption Algorithm, ..399
Internet, ...128
manipulaciones IP, ...54
peligros, ...123
Internet Control Message Protocol, ...53
Internet Explorer
Active Setup, ...149
ajustar niveles de seguridad, ...132
asistente para perfiles, ...138
aviso de cookie, ...474
caché de Internet, ...329
certificados, ...136
concepto de seguridad, ...127
conexiones seguras, ...137
Cookie Pal, ...477
cookies, ...470
desactivar ActiveX, ...154
desactivar Java, ...157
desactivar JavaScript, ...162
desactivar VisualBasicScript, ...165
función de historial, ...334
identificar la zona de seguridad, ...129
niveles de seguridad, ...129
opciones de seguridad avanzadas, ...135
PlugIns desactivar, ...167
proteger las direcciones de e-mail, ...484
protocolos de seguridad, ...138
redirigir datos de formularios, ...139
sitios web en zonas de seguridad, ...133
Stealth Anonymizer, ...492
zonas de seguridad, ...128
Internet Protocol, ...546
Internet Relay Chat, ...546
Interpretador, ...546
Intranet, ...546
Intranet Local, ...128
Intrusion Detection System. ....Véase IDS
Investigación personal, ...454
buscadores, ...454
Investigación sobre personas
metabúsqueda, ...455
IP, ...546
IP-Spoofing, ...54, 546
IRC, ...546
ISDN, ...550
ISP, ...545

J

Jaula de Faraday, ...118
Java, ...156, 546
concepto de seguridad, ...156
desactivar, ...157
JavaScript, ...160, 547
desactivar, ...162
testear, ...161

K

Kevin Mitnick, ...17
Keyserver, ...401

L

LAN, ...547
Linux, ...523
base de datos de hardware, ...527
costes, ...524
daemon de Internet. Véase inetd
desinstalar el paquete de software, ...533
hardware, ...526
inetd, ...528
inetd.conf, ...532
manejo, ...525
protegerlo, ...528
servicios de red, ...528
software, ...526
Linux yast, ...528
Listas de correo, ...547
Listas de mailing
list-linking, ...376
List-linking, ...376

M

Manipulaciones IP, ...54
Mayúsculas/minúsculas, ...105
Medios de memoria intercambiable, ...67

MESA, ...459
MetaEmailSearchAgent, ...459
MetaGer, ...455
Meta-tags, ...507
Microsoft
  Active Setup, ...149
  Authenticode, ...153
  VisualBasicScript, ...164
MIME, ...547
Módem, ...547
Monitor
  radiación, ...117

N

Navegación anónima, ...481
Navegador, ...548
Navegador web
  adaptarlo para Cookie Pal, ... 477
  agujeros de seguridad, ... 146
  Bookmarks, ...328
  caché de Internet, ... 327
  Complete Cleanup, ...337
  cookies, ...469
  cookies previa consulta, ...473
  favoritos, ...328
  función de historial, ... 328
  history, ...328
  huellas de navegación, ...326
  señaladores de lectura, ...328
  testear anonimato, ...482
  verificar, ...146
Navegadores web, ...127
Navegar
  anónimamente, ...481
Navegar por la Red
  anónimamente, ...481
NeoTrace, ...26, 276, 286
  datos de emplazamiento, ...277
  seguimiento de las conexiones, ...279
  Whois, ...282
Netiquette, ... 548
Netscape Navigator, ...548
  activar cifrado, ...139
  aviso de cookie, ...474
  caché de Internet, ... 333
  concepto de seguridad, ...139
  conexiones seguras, ...140
  contraseñas guardadas, ... 145
  Cookie Pal, ...478
  cookies, ... 471
  desactivar Java, ... 159
  desactivar JavaScript, ...162
  estado de la conexión, ...143
  History, ...336
  proteger la dirección de correo electrónico, ...144
  proteger la dirección de e-mail, ...485
  SmartUpdate, ...150
  Stealth Anonymizer, ...493
Network File System, ...49
NFS, ...49
Nivel de inclusión, ...502
Niveles de seguridad, ...129
  ajuste individual, ...132
NNTP, ... 235
Nombres IP, ... 548
NSA, ...548
Número IP, ... 269

O

Ofertas web
  analizarlas, ...499
Office
  contraseña, ...111
OfficePassword, ... 111
Outlook Express, ...82
  desencriptar mensajes, ...420
  firmar mensajes, ...421
  inmunizarlo contra virus, ...383
  Plug-In de PGP, ...404
  S/MIME, ...432
  verificar firmas, ...424
  visualizar información de la cabecera, .392
  visualizar la cabecera, ...392

P

Packet Internet Groper. Véase Ping
Páginas web
  áreas protegidas, ...514
  manipulación, ... 511
  protegerlas, ...507
Palabra clave. ....Véase contraseña
Parches, ...46
PassKeeper, ...339
Passphrase, ...409
Password-Sniffing, ...51
Patch, ...549
PC autónomo, ... 67
PC Spy, ...259
  activar, ...263
  analizar las grabaciones, ...263
  opciones de pantalla, ...261

PCT 1.0, ...138
Perfiles de usuario, ...75
Persecución por vía penal, ...295
Personal Firewall, ...268
Personal Web Server, ... 357
PGP, ...402, 404, 549
asistente de creación de claves, ...406
con cualquier aplicación, ... 424
crear clave, ... 406
desencriptar mensajes, ... 420
distribuir claves, ...412
encriptar mediante el portapapeles, ... 425
fiabilidad, ...430
firmar mensajes, ...421
importar clave, ... 415, 416
incluir clave, ...415
longitud de la clave, ...408
passphrase, ... 409
PGPkeys, ... 410
PGPTray, ...425
plug-in para Outlook Express, ... 404
publicar la clave, ...413
seguridad, ...430
servidor de claves, ...410
servidores de claves, ...413
verificar firmas, ...424
vigencia de la clave, ...409
Ping, ...27, 268
Pinger, ...28, 37
Plug-in, ...549
PlugIns, ...166
desactivar, ...167
desinstalar, ...168
Medidas de prevención, ...167
Port, ...187, 301
Ports, ...30
Portscans, ...30, 218, 301
detectar troyanos, ...187
legalidad, ...295
YAPS, ... 302
PPP, ... 549
Pretty Good Privacy. ....Véase PGP
Private Communications Technology, ... 138
Private Idaho, ...366
Protección contra virus, ...169
Protocolos, ...249
Protocolos de red, ...354
Protocolos de seguridad, ...138
Public Key, ...550
Publicidad, ...126
Puertos, ...233
Puntos débiles, ...17

R

Radiación electromagnética, ...116
Recursos legales, ...295
derecho civil, ...296
derecho penal, ...295
Redes, ... 299
atacar el tráfico de datos, ...315
enlaces entre protocolos, ...355
exploración, ... 27
protección contra virus, ...172
protocolos, ...354
Sniffing, ...315
tarjetas de red, ...315
Redirigir datos de formularios, ...139
RFCs, ...550
Rhino9, ...37
Riesgos financieros, ... 126
Routing, ...550
RPV, ...550
RSA, ... 401, 407, 551

S

S/MIME, ...430
desencriptar, ...433
distribuir certificado, ...432
encriptación y firma, ...433
generar certificado, ...431
Sabotaje, ...64
Denial of Service, ...52
Sabotaje informático, ...296
Salus, ...249
activar, ...250
analizar el protocolo, ...252
contraseña, ...252
desactivar, ...258
entradas por teclado, ...255
espiar contraseñas, ...256
modo invisible, ...253
Salvapantallas, ...94
activación manual, ...97
averiguar contraseña, ...100
cualquier programa como, ...100
forzar, ...97
protección por contraseña, ...94
proteger, ...98
seguridad, ...97
seguros, ...99
Sandbox, ...194
SATAN, ...551
Scans antivirus

con temporizador, ...181
Scans antivirus manuales, ...176
Screen Saver Destroyer 2000, ...97
Scripts, ...160
Secret Key, ...551
Secure Multipurpose Internet Mail Extension, .430
Secure Socket Layers, ...138, 140
Servidores de claves,.... 401
Service Pack, ...551
Servicios de red, ...528
Servidor, ...25, 551
Servidor de correo,.... 552
Servidor de entrada de correo, ...552
Servidor de salida de correo,.... 552
Servidor de teletransmisión de datos, ...359
Servidor Proxy, ...552
Servidor web, ...552
ataques, ...516
SET, ...552
Shell, ...552
Shell-Script, ...553
S-HTTP, ...399, 402, 553
Simétrica
encriptación, ...553
Simétrica (encriptación), ...397
Simple Mail Transfer Protocol. ....Véase SMTP
Sistema operativo
alternativas, ...519
averiguar, ...34
Sistemas operativos
agujeros de seguridad, ...45
fallos del sistema, ...45
Sitios de confianza, ...128, 134
Sitios restringidos, ...128
Sitios web
en zonas de seguridd, ...133
Script-kids, ...59
SLIP, ...553
SmartUpdate, ...150
SMTP, ...204, 390, 553
Sniffer, ...553
Sniffing, ...51, 315
Sniffing de paquetes, ...51, 315
SpyNet, ...316
Sobreacoplamiento, ...120
Social Engineering, ...56, 554
Social Hacking, ...56, 554
Software
desconocido, ...191
detección, ...33
testear, ...191
Software Anonymizer, ...490
Soporte de datos, ...68
Soportes de datos
medidas de prevención, ...170
Source Route Option, ...55
SpyNet, ...316
CaptureNet, ...316
PeepNet, ...319
SSL, ...138, 140, 399, 402, 554
Standard-Disclaimer, ...325
Stealth Anonymizer, ...490
Steganos, ...436
ocultar datos, ...437
volver visibles los datos, ...440
Subredes, ...29
Suma de comprobación, ...75, 554
Supervisor de la red, ...352

T

Tarifa plana, ...301
Tarjetas de red, ...315
TCP, ...554
TCP/IP, ...26, 204, 233, 301
manipulaciones IP, ...54
secuestro de conexiones, ...55
Teclado, ...67
Teleport Pro, ...500
Teletransmisión de datos, ...555
Telnet, ...36, 48
TEMPEST, ...116, 555
software de protección, ...119
TLS,.... 138, 140
T-Online, ...555
Traceroute, ...271, 555
NeoTrace, ...276
tracert, ...26, 271
Transport Layer Security, ...138
Triple-DES, ...399
Troyanos, ...32, 42, 125, 185, 555
BackOrifice, ...43
detectar, ...185
encontrarlos en ficheros, ...189
erradicar, ...191
verificar el registro, ...188

U

UDP, ...556
Unidades de disquete
protección, ...172
Unix, ...35, 82, 556. Véase Linux
derechos de ficheros, ...513

Usenet, ...556
Uso compartido de ficheros
darle seguridad, ...348
desactivar, ...347
verificar el estado, ... 346
Uso compartido de ficheros e impresora, ..345
UUCP, ...556

V

VBScript. .....Véase VisualBasicScript
VeriSign, ...431
Vigilancia, ...248
aplicaciones, ...249
en el puesto de trabajo, ...321
en la empresa,..... 322
legalidad, ...322
óptica, ...259
óptica y acústica, ...115
PC Spy, ...259
PCs no custodiados, ...259
posibilidades técnicas, ...322
protocolos, ...249
radiación electromagnética, ...116
Salus, ...249
sobreacoplamiento, ...120
Vigilancia en el puesto de trabajo, ...321
Virus, ...381, 556
hoax,..... 389
por correo electrónico, ...381
Virus de test, ...173
Virus informáticos, ...41, 124, 169, 556
en redes, ...172
escáner de segundo plano, ...173
evitar infecciones, ...170
scans con temporizador, ...181
scans manuales, ...176
virus de test, ...173
VisualBasicScript, ...164
desactivar, ...165
vmyths.com, ...389

W

Webbrowser
contenidos activos, ...152
PlugIns, ...166
Whois, ...272, 282
Windows
Active Setup, ...149
administrador de usuarios, ...75
alternativas, ...519
arranque de sesión, ...78
desactivar el uso compartido, ...347
enlaces entre protocolos, ...355
entorno de red, ...346
esquivar el registro, ...84
NT/2000, ... 82
protocolos de red, ...354
registro, ...188
salvapantallas, ...94
servidor de teletransmisión de datos, ...359
supervisor de la red, ...352
uso compartido de ficheros con seguridad, ...348
uso compartido de ficheros e impresora, ...49, 345
verificar el uso compartido de ficheros, 346
Windows NT/2000, ...519
administrador de usuarios, ...522
hardware, ...521
software,..... 521
WinSafe, ...99
Word
contraseña, ...111
WS_FTP Pro, ...512

Y

YAPS, ...30, 302
analizar resultados, ...306
configurar, ...303
realizar portscan, ...305
Yast, ...528

Z

Zero Emission Pad, ...119
Zona de seguridad
asignar sitios web, ...133
Zonas de seguridad, ...128, 213, 383
ZoneAlarm, ...207, 286
Alarmas, ...217
AlertAnalyzer, ...218
controlar las alarmas, ... 218
controlar las aplicaciones, ...210
definir reglas,..... 211
eludir Internet Lock, ...217
fichero de protocolo, ...220
Función de cuarentena, ...215
Instalación, ...207
Internet Lock, ...215
MailSafe, ... 215
módulo de control, ...209
zonas de seguridad, ...213